

# Windows IT Pro

APRIL 2010 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU



## Defuse IT Annoyances

- 4 Patch Management Problems p. 21
- 9 Windows 7 Woes p. 25
- 5 Active Directory Headaches p. 28
- 7 Hyper-V Idiosyncrasies p. 31
- 4 Failover Clustering Hassles p. 33
- 5 SharePoint Frustrations p. 36

**Mark Minasi's  
Windows Power Tools p. 11**

**Prepare to Deploy  
Exchange 2010 p. 44**

**Top 10:  
Office 2010 Features p. 13**

**Get Information  
About .msi Files p. 47**

**Microsoft Deployment Toolkit:  
Migrate XP to Windows 7 p. 39**

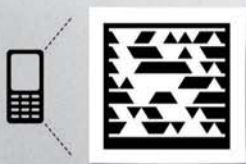
**Required Reading:  
SQL Server on  
Hyper-V p. 49**



*Drive efficiency and fuel  
inspiration where it strikes.*


Windows® 7 Enterprise Edition, Windows Server® 2008 R2, Microsoft® System Center and Forefront™ can help drive the success of your business. How, exactly? Well, when deployed together, they help streamline management of your desktops, minimize threats and data loss, while maximizing secure remote access and user productivity across applications, locations and devices. End result? Inspired users. Efficient business. Happy IT.

To learn more about the benefits of these products, go to [itseverybodysbusiness.com/deploy](http://itseverybodysbusiness.com/deploy)



Snap this tag to get the latest news  
on deploying optimized desktops  
or text DEPLOY to 21710\*

Get the free app for your phone at  
<http://gettag.mobi>

Because it's everybody's  business



## COVER STORY

## Defuse IT Annoyances

**21** Solve 4 Common Patch Management Problems

Use these tips to help find which updates have been deployed, prevent update traffic from saturating WAN links, prevent end-user interruptions, and establish a group of update testers.

BY ORIN THOMAS

**25** 9 Workarounds for Windows 7 Woes

If you're looking for a way to deal with some of Windows 7's compatibility or automatic reboot issues or you simply want to change a taskbar, Start menu, or Windows Explorer feature back to the way it was, fear not: We've got your back.

BY PAUL THURROTT

**28** Soothe 5 Active Directory Headaches

Active Directory has its share of annoyances; some solutions require upgrading to Windows Server 2008, but sometimes the right knowledge lets you work around AD's problems.

BY SEAN DEUBY

**31** Prepare Now For 7 Hyper-V Migration Idiosyncrasies

Learn about Hyper-V's pitfalls before making the move.

BY ALAN SUGANO

**33** 4 Failover Clustering Hassles and How to Avoid Them

Failover clustering was difficult and frustrating before, but with Windows Server 2008, it's gotten much easier. Learn how it's changed.

BY JOHN SAVILL

**36** 5 SharePoint Frustrations You Can Overcome

If you've deployed SharePoint 2007, you've probably been discouraged by minor frustrations associated with the technology. Here are five of the most common problems and recommended workarounds.

BY MICHAEL NOEL

## FEATURES

## SOLUTIONS PLUS

**39** XP to Windows 7 Migration with Microsoft Deployment Toolkit 2010

Follow these step-by-step instructions to get your Windows XP machines migrated to Windows 7 quickly and easily with help from a powerful Microsoft tool.

BY RHONDA LAYFIELD

**44** Preparing to Deploy Exchange 2010

Before installing Microsoft Exchange Server 2010, you need to be sure you're on a supported OS and that your infrastructure and hardware meet the requirements. Also get to know your current system and the new capabilities of Exchange 2010.

BY TONY REDMOND

**47** Get Information About .msi Files with Just a Few Clicks

If you have an .msi file with an obscure filename, you can find out what software program it will install without using Orca or having to run it on a test machine. Here's a utility that will retrieve the program's name, version, and more.

BY BILL STEWART

## REQUIRED READING: VIRTUALIZATION

**49** Make SQL Server Sing on Hyper-V

Production SQL Server 2008 instances are prime candidates for running in a virtual machine. And Windows Server 2008 R2 Hyper-V is the best virtualization application Microsoft has produced to date for supporting mission-critical, resource-intensive server applications such as SQL Server. In this article, Wendy Henry introduces you to the key concepts and whets your appetite to learn more about these powerful tools.

BY WENDY HENRY

## IN EVERY ISSUE

**6** IT Community Forum**71** Directory of Services**71** Advertising Index**71** Vendor Directory**72** Ctrl+Alt+Del

## Windows IT Pro

A PENTON PUBLICATION

APRIL\_2010

VOLUME\_16

NO\_4

## COLUMNS

## CROCKETT | IT PRO PERSPECTIVE

**5** Join the Windows IT Pro Team

Windows IT Pro has launched new initiatives that let IT pros contribute to content planning.

## THURROTT | NEED TO KNOW

**8** What You Need to Know About Microsoft Desktop Optimization Pack 2009 R2

Microsoft Desktop Optimization Pack (MDOP) is an unparalleled collection of tools and

technologies that includes two desktop virtualization products, error monitoring, asset inventory, and more.

## MINASI | WINDOWS POWER TOOLS

**11** Formatting and Resizing Partitions with Diskpart

Learn how to use Diskpart to format disk partitions, assign them drive letters, and even shrink and expand them.

## OTEY | TOP 10

**13** New Features in Office 2010

Microsoft Office 2010 comes with a 64-bit version and includes other improvements for security and productivity such as new image editing in Word and PowerPoint and coauthoring of documents.

## INTERACT

**14** Reader to Reader

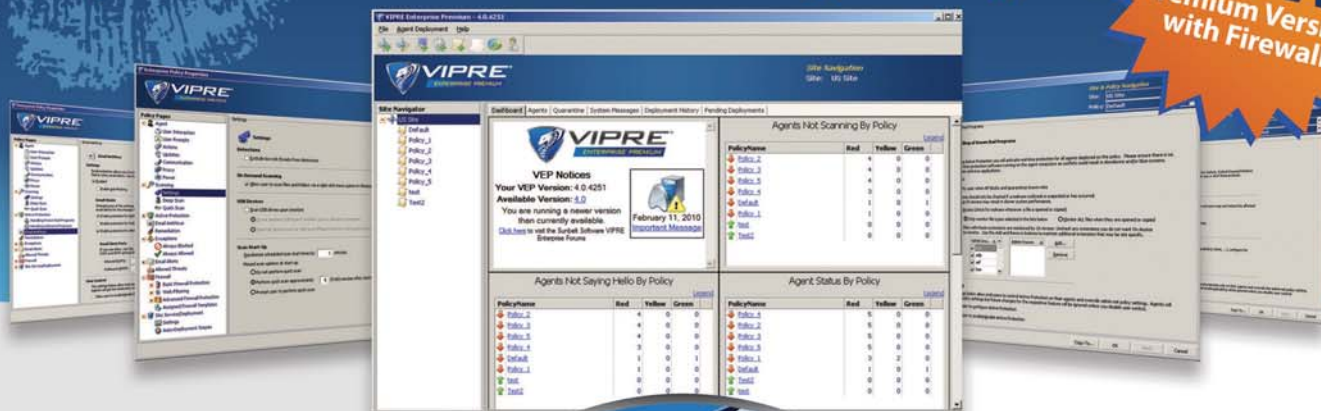
Run and create virtual machines with the free VMware Player 3.0 and customize the PowerShell console's colors.

**18** Ask the Experts

Learn to create Outlook Quick Parts, create SAN certificates, turn jumbo frames on in Hyper-V, and more.

# Kiss your antivirus bloatware goodbye

**NEW**  
Premium Version  
with Firewall

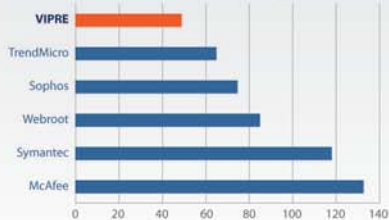


# VIPRE

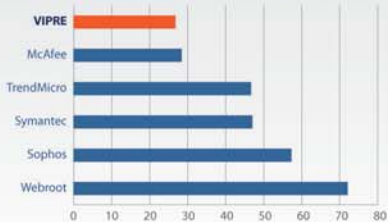
TEST DRIVE

ENTERPRISE PREMIUM

Memory Used During Scan



CPU % Used During Scan



How does your current software compare?

VIPRE Enterprise scans at a brisk 13.95 MB/sec and uses just 27% of CPU and 50 MB of RAM. In idle, it uses a mere 13.3 MB RAM with a disk footprint of just 113 MB. You'll hardly notice it's running!

## Special Competitive Upgrade: 50% Discount!

Until now, antivirus engines have been Franksteins, bolted together from bits and pieces of different products. They're slow, full of bugs, and hard to manage.

VIPRE Enterprise Premium is a revolutionary new approach. It combines high-performance antivirus, antispyware, and desktop firewall into a single agent so you get comprehensive endpoint malware protection with low system resource usage. It's fast, powerful and easy.

Plus, advanced anti-malware technology protects your system against the new wave of malware threats. No more juggling multiple programs. No more dealing with user complaints about slow workstation performance.

- **COMPLETE!** All-in-one protection from today's malware.
- **FAST!** High-performance and low impact on system resources.
- **EASY!** Manage everything easily from one command screen.
- **RELIABLE!** Configurable, real-time monitoring technology.
- **AFFORDABLE!** Ask for a quote with our 50% competitive upgrade discount!

Why struggle with slow resource hogs when you can manage ALL your malware threats with one fast, easy application?

**Curious? Download your FREE copy of VIPRE Enterprise Premium and give it a test drive.**

When you compare VIPRE Enterprise Premium to Symantec, McAfee, Trend Micro or whatever antivirus program you're using, **you WILL want to switch!** Don't worry, though. You can get VIPRE Enterprise Premium with a **50% competitive upgrade discount!**



Sunbelt Software

**Plus we will buy out your existing maintenance contract for 1 year!**

Download now: **www.TestDriveVipre.com**

Sunbelt Software Tel: 1-888-688-8457 or 1-727-562-0101 Fax: 1-727-562-5199 [www.SunbeltSoftware.com](http://www.SunbeltSoftware.com) [sales@sunbeltsoftware.com](mailto:sales@sunbeltsoftware.com)

© 2010 Sunbelt Software. All rights reserved. VIPRE Enterprise is a trademark of Sunbelt Software. All trademarks used are owned by their respective owners.

Discount available on new licenses only for a limited time. Buy-out offer good on contracts up to 1 year. Subject to change without notice. Contact your Sales Representative for details.



## PRODUCTS

### 56 New & Improved

Check out the latest products to hit the marketplace.

**PRODUCT SPOTLIGHT:** NitroSecurity *NitroView Enterprise Security Manager*

#### REVIEW

### 57 Paul's Picks

Windows 7 antipiracy technology—should you care? And why you might hold off on buying the iPad.

BY PAUL THURROTT

#### REVIEW

### 58 Automation Anywhere 5.5 Enterprise

Automation Anywhere does just what its name suggests, offering IT pros the ability to automate a wide range of chores—but what it really delivers is the ability to simplify your job.

BY MEL BECKMAN

#### REVIEW

### 59 WMIX 2.0

With WMIX 2.0, you can use a GUI to write custom scripts and queries that access computer information with Windows Management Instrumentation (WMI).

BY BRANDON CARSE

#### REVIEW

### 60 Splunk 4.0

Splunk collects and indexes event data so that you can easily search it the next time you're looking for the cause of a problem.

BY BRANDON CARSE

#### COMPARATIVE REVIEW

### 61 2 Tools to Restore Active Directory Objects

These two Active Directory products offer an alternative to the AD recycle bin by providing AD object restore—and more.

BY ERIC B. RUX

#### BUYER'S GUIDE

### 65 Windows Password Reset Products

Incredibly, 25 percent of Help desk calls are to reset users' passwords. Get a self-service product, and turn this task over to your users.

BY LAVON PETERS

### 67 Industry Bytes

See why the introduction of the Ribbon in SharePoint 2010 is a big win; create professional HTML resumes; and chime in on which smartphones are best for the enterprise.

## Windows IT Pro

### EDITORIAL

#### Editorial and Custom Strategy Director

Michele Crockett mcrockett@windowsitpro.com

#### Executive Editor, IT Group

Amy Eisenberg amy@windowsitpro.com

#### Technical Director

Michael Otey motey@windowsitpro.com

#### Senior Technical Analyst

Paul Thurrott news@windowsitpro.com

#### Custom Group Editorial Director

Dave Bernard dbernard@windowsitpro.com

#### Web and Developer Strategic Editor

Anne Grubb agrubb@windowsitpro.com

#### Systems Management

Karen Bemowski kbemowski@windowsitpro.com

Caroline Marwitz cmarwitz@windowsitpro.com

Zac Wiggy zwiggy@windowsitpro.com

#### Messaging, Mobility, SharePoint, and Office

Brian Keith Winstead bwinstead@windowsitpro.com

#### Networking and Hardware

Jason Bovberg jbovberg@windowsitpro.com

#### Security

Lavon Peters lpeters@windowsitpro.com

#### SQL Server

Megan Bearly Keller mkeller@windowsitpro.com

Sheila Molnar smolnar@windowsitpro.com

#### Production Editor

Brian Reinholz breinholz@windowsitpro.com

#### IT Media Group Editors

Linda Harty, Chris Maxcer, Rita-Lyn Sanders

### CONTRIBUTORS

#### SharePoint and Office Community Editor

Dan Holme danh@intelliem.com

#### Senior Contributing Editors

David Chernicoff david@windowsitpro.com

Mark Joseph Edwards mje@windowsitpro.com

Kathy Ivens kiven@windowsitpro.com

Mark Minasi mark@minasi.com

Paul Robichaux paul@robichaux.net

Mark Russinovich mark@sysinternals.com

#### Contributing Editors

Alex K. Angelopoulos aka@mvps.org

Sean Deuby sdeuby@windowsitpro.com

Michael Dragone mike@mikerochip.com

Jeff Felling jeff@blackstatic.com

Brett Hill brett@iisanswers.com

Darren Mar-Elia dmarrelia@windowsitpro.com

Tony Redmond tony.redmond@hp.com

Ed Roth eroth@windowsitpro.com

Eric B. Rux ericrux@whshelp.com

John Savill john@savilltech.com

William Sheldon bsheldon@interknowlogy.com

Randy Franklin Smith rsmith@montereytechgroup.com

Curt Spanburgh cspanburgh@scg.net

Orin Thomas orin@windowsitpro.com

Douglas Toombs help@toombs.us

Ethan Wilansky ewilansky@windowsitpro.com

### ART & PRODUCTION

#### Production Director

Linda Kirchesler linda@windowsitpro.com

#### Senior Graphic Designer

Matt Wiebe matt.wiebe@penton.com

### ADVERTISING SALES

#### Publisher

Peg Miller pmiller@windowsitpro.com

#### Director, International and Agency Services

Don Knox don.knox@penton.com

#### EMEA Managing Director

Irene Clapham irene.clapham@penton.com

#### Director of IT Strategy and Partner Alliances

Birdie J. Ghiglione birdie.ghiglione@penton.com, 619-442-4064

#### Online Sales and Marketing

##### Manager

Dina Baird Dina.Baird@penton.com

#### Key Account Directors

Jeff Carnes jeff.carnes@penton.com 678-455-6146

Chrissy Ferraro christina.ferraro@penton.com 970-203-2883

#### Account Executives

Barbara Ritter barbara.ritter@penton.com 858-759-3377

Cass Schulz cassandra.schulz@penton.com 858-357-7649

#### Client Project Managers

Michelle Andrews 970-613-4964

Kim Eck 970-203-2953

#### Ad Production Supervisor

Glenda Vaught glenda.vaught@penton.com

### MARKETING & CIRCULATION

Customer Service service@windowsitpro.com

#### IT Group Audience Development Director

Marie Evans marie.evans@penton.com

#### Marketing Director

Sandy Lang sandy.lang@penton.com

### CORPORATE



#### Chief Executive Officer

Sharon Rowlands Sharon.Rowlands@penton.com

#### Chief Financial Officer/Executive Vice President

Jean Clifton jean.clifton@penton.com

### TECHNOLOGY GROUP

#### Senior Vice President, Technology Media Group

Kim Paulsen kpaulsen@windowsitpro.com

Windows®, Windows Vista®, and Windows Server® are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries and are used by Penton Media under license from owner. *Windows IT Pro* is an independent publication not affiliated with Microsoft Corporation.

#### WRITING FOR WINDOWS IT PRO

Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

#### PROGRAM CODE

Unless otherwise noted, all programming code in this issue is © 2009, Penton Media, Inc., all rights reserved. These programs may not be reproduced or distributed in any form without permission in writing from the publisher. It is the reader's responsibility to ensure procedures and techniques used from this publication are accurate and appropriate for the user's installation. No warranty is implied or expressed.

#### LIST RENTALS

Contact Walter Karl, Inc. at 2 Blue Hill Plaza, 3rd Floor, Pearl River, NY 10965 or www.walterkarl.com/mailings/pentonLD/index.html.

#### REPRINTS

Diane Madzelonka, Diane.madzelonka@penton.com, 216-931-9268, 888-858-8851

Experience a whole new level  
of system speed and efficiency



by *preventing* fragmentation  
*before* it happens.

**NEW**  
**Diskeeper**  
2010

Try it now at  
[www.diskeeper.com/special45daytrial](http://www.diskeeper.com/special45daytrial)



© 2009 Diskeeper Corporation. All Rights Reserved. Diskeeper, "the only way to prevent fragmentation before it happens", Intelliwrite, Clean Disk logo and Diskeeper Corporation logo are registered trademarks owned by Diskeeper Corporation in the United States and other countries. All other trademarks and brand names are the property of their respective owners.

"We're stepping up our efforts to gather feedback from our IT pro audience."



## Join the *Windows IT Pro* Team

New initiatives let you sound off about IT topics

**A**re you a Hyper-V person or an ESX person? PC or Mac? Or are you staunchly brand-disloyal, particularly when you're buying hardware and software on a tight budget—figuring that whatever works and costs the least will win the bid?

We at *Windows IT Pro* want to know what your IT department's process is for selecting products and services. Does your company tend to stick to certain brands? Do you have a formal evaluation process, or do you go with your gut? Who ultimately makes the IT buying decisions? What do you wish you could change about the process?

The IT buying process will be the first topic of our new monthly survey series that will help us plan content for the magazine, email newsletters, and website. You can find a link to the survey at [www.windowsitpro.com/go/perspectives](http://www.windowsitpro.com/go/perspectives). We'll change the survey topic frequently, so be sure to visit the IT Pro Perspectives link often. Every time you respond to one of our surveys, you'll be entered in a drawing for some cool prizes ("cool" being a relative term in these budget-conscious times).

Launching the monthly survey process is one way we're stepping up our efforts to gather feedback from our IT pro audience. We've always conducted surveys and sifted through letters, article comments, Instant Polls, and discussion forum posts to determine what problems IT pros grapple with so we can plan our content. As an example, reader feedback is the primary driver of the topics we covered this month in our "IT Annoyances" articles.

But with the launch of the IT Pro Perspectives site, we now offer a much more interactive forum for you to share your opinions. We'll feature results of our reader surveys so you can compare your feedback with that of your peers. We'll highlight some of the most compelling comments to articles. We'll also ask you to rate proposed topics for product coverage, buyer's guides, and feature articles, and suggest other article topics.

If this involvement just whets your appetite for more, we have additional opportunities for you to join the *Windows IT Pro* team. We're now accepting applications from readers who would like to participate in our *Windows IT Pro* Advisory Board, a virtual gathering of editors, readers, user group leaders and members,

vendor technical representatives, and authors. The Advisory Board will meet monthly by phone to share observations about the industry, compare trends, and suggest initiatives that *Windows IT Pro* can undertake on behalf of the IT pro community.

And finally, for those who have the rare combination of IT experience and writing skills, we've launched our "Blogger of the Month" program, which will feature a weekly blog written by one of our readers whose winning entry was selected by our panel of editors. To enter, simply write and upload a sample blog expressing

your opinion about any IT topic or offering some tips or observations to your fellow IT pros. If your entry is selected, you'll get to hold forth in a weekly blog on the *Windows IT Pro* site for a month—to a potential audience of about 2.5 million per month.

As we reach the midpoint of our 15<sup>th</sup> year of publication, we extend our thanks to every reader who's ever commented on an article, pointed out our mistakes, disagreed with a product assessment, or told us that we helped him get his job done. We

not only appreciate the feedback—we depend on it to produce content that's relevant to you. We're eager to see the results of our new Perspectives site, because we suspect that the easier and more interactive we make our communication with you, the better information we'll get.

We appreciate the praise such as the note we recently received from CIS instructor Eric Magidson, who wanted to inquire about multiple copies of a recent issue for his students: "I have been an avid subscriber of *Windows IT Pro* for many years and feel that it is, by far, the best magazine and investment my students can make."

But we know we don't always get it right. Help us serve up even better content by adding your voice—in any number of ways—at [www.windowsitpro.com/go/perspectives](http://www.windowsitpro.com/go/perspectives). You can start today by responding to our current survey about how you evaluate and purchase IT products and services.



InstantDoc ID 103601

We appreciate your feedback, and we depend on it to produce relevant content.

**MICHELE CROCKETT** ([michele.crockett@penton.com](mailto:michele.crockett@penton.com)) helped launch *SQL Server Magazine* in 1999, has held various business and editorial roles within Penton Media, and is currently editorial and custom strategy director of *Windows IT Pro*, *SQL Server Magazine*, and *System iNEWS*.

■ PowerShell Editors  
■ System Uptime

■ Smartphone Choice  
■ Exchange Migration

## LETTERS@WINDOWSITPRO.COM

### Pair of PowerShell Editors Pack a Punch

Thanks for the great review in "Pair of PowerShell Editors Pack a Punch" (March 2010, InstantDoc ID 103483)! I have one correction: PrimalScript has always offered block selection. Just hold down the Alt key while making a selection, and you can select a block of text. Then, use the standard copy and paste commands.

—Ferdinand Rios, CEO, SAPIEN Technologies

### System Uptime

Regarding John Savill's FAQ, "What's a fast way to find how long my system has been running?" (February 5, 2010, InstantDoc ID 103540), I'd like to offer another option. I've been using uptime.exe (support.microsoft.com/?kbid=232243) for years, and it still works great. It even returns uptime info for remote machines.

—Paul Smith

Since Windows NT 4.0, Task Manager has offered a way to determine how long a system has been running. Go to the Processes tab, then click View, Select Columns. Select CPU Time, and click OK. Now, click the CPU Time column header to sort the results in descending order. At the bottom, look for System Idle Process. (You might need to select *Show processes from all users* to display System Idle Process.)

—Frank Bernard

### Choosing a Smartphone

I've enjoyed reading Brian Winstead's series "Choosing a Smartphone" (InstantDoc IDs 103578, 103505, and 103473), in which he walks through the decision-making process. At work, I've been in the same process for several months. All the factors in Brian's article are important, and I'd like to offer a few more.

I think smartphone use (regardless of OS or UI) is a generational and therefore

personal choice. Consider the recent market theory that a business person will likely put up with carrying only two devices. We're all "information workers," despite our titles, so there's a high probability we're already carrying a laptop (or netbook). That leaves us with one more device. We could cope with the limitations of a netbook (or tablet) as our only device (with 3G connectivity), but many people want a pocket-sized one that gives them universal connectivity.

If you're part of the younger generation, you probably love your smartphone. It makes your job fun and keeps things interesting. The more apps it contains, the higher its coolness factor, the better the experience, and the more fun you have working. But if you're part of the older generation (as I am), you don't really care about a smartphone that's crammed with apps. You just want a phone! Yes, I use an HTC Windows Mobile smartphone, but can I live without it? Yes!

My company will support both types of users, and it's easy to provide such multifaceted support with Exchange. We won't require our employees to use smartphones, and we won't provide them, either. But we'll probably subsidize mobile devices to a certain point and let staff use the devices that make them happy. We look forward to the productivity benefits of users finding new enjoyment in getting their work done.

—Jim Wirthlin

*You raise some excellent points—particularly about the generational split surrounding smartphones, something I hadn't really considered. I do wonder whether that has anything to do with why more IT shops are giving users more choice of mobile devices these days rather than supporting a single mobile platform.*

*As for myself, I fall somewhere between the mainframe generation and the digital natives. I'm seduced by the coolness factor*

### Migrating to Exchange 2010

Brian Winstead anticipates the launch of Exchange Server 2010 in "Exchange 2010: The Migration Story" (October 2009, InstantDoc ID 102892). My company is considering a migration to Exchange 2010; we're currently running Exchange 2003, and the need for high availability has come into the equation. Therefore, moving to a new version of Exchange is the way to go.

Hardware requirements will indeed be a consideration. However, at this stage, our need for the new product's features outweighs hardware cost. Do you know of many companies that have accomplished the migration? Can you provide any tips in terms of hurdles encountered throughout the implementation/deployment process?

—Ian Salgado

*Thank you for writing! If you're looking to implement high availability, Exchange 2010's Database Availability Group (DAG) approach looks like a cost-effective option. If you haven't read Tony Redmond's article "Exchange 2010: High Availability with DAGs" (InstantDoc ID 102925), I recommend that you check it out. Regarding companies already using Exchange 2010, you can find a collection of case studies on Microsoft's website ([www.microsoft.com/exchange/2010/en/us/case-studies.aspx](http://www.microsoft.com/exchange/2010/en/us/case-studies.aspx)). Click a company logo for details about each case. Also, our May cover story will walk through the upgrade from Exchange 2003 to Exchange 2010. Let me know how your project goes!*

—Brian Keith Winstead

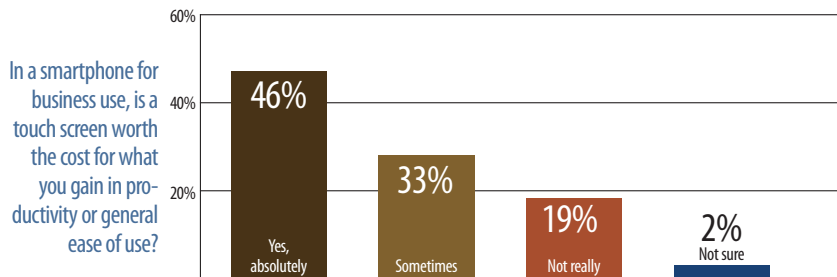
*while remaining unsure whether I'll use all those cool features or adjust to that all-the-time access. As I mentioned in the first article of this series, I've never owned a cell phone, and that's largely because I rather enjoy being unavailable! But we'll see how it goes, and you can bet I'll be writing more about my experiences with the device I end up choosing.*

—Brian Keith Winstead

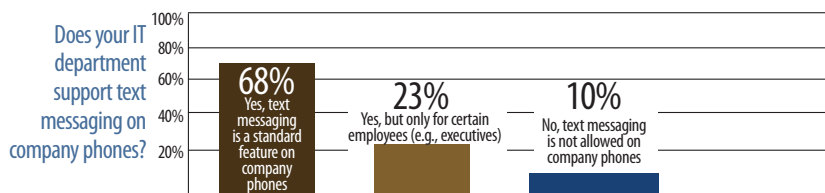
Windows IT Pro welcomes feedback about the magazine. Send comments to [letters@windowsitpro.com](mailto:letters@windowsitpro.com), and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.



## Instant Poll Results: Touch Screens



## Instant Poll Results: Text Messaging



## Windows IT Pro Forums

[www.windowstipro.com/forums](http://www.windowstipro.com/forums)

*Readers are interacting online in our forums. Here, we present excerpts of their comments in their own words.*

Forums > Terminal Server/  
Terminal Services

[A client I work with has] a few hundred users and two IT on staff. They have a terminal server that at least half the staff uses over the course of the day. One user is suddenly getting an Access Denied for the roaming profile, and then an error with the local profile. Problem is, they stopped using roaming profiles over eight months ago, going with two programs, ScriptLogic and Desktop Authority (both of which I know nothing about). The user is definitely NOT pointing to a roaming profile. The user has logged on to other PCs throughout the facility with NO issues.

Here is what I've done so far: I renamed and recreated the local profile; this seemed to work. I logged on and off the terminal server multiple times to make sure it held together, and it did. When I told the onsite IT admin to configure whatever else he needed on the profile, he emailed me back saying what I did didn't work.

When I logged back on he had deleted the old profile and renamed the new one, but when I tried to log in as the affected user I got the errors again. I backed up the newer profile and deleted, but it still gives the error and will not create a new local profile. I also tried adding a roaming profile and logging in, but the

errors still came up, I've since removed the roaming profile so as to not affect the user elsewhere. I've checked the local policy settings. I've checked to see if a local user was set up in the domain user's name. Nothing. Any ideas that I'm missing? Oh, and the terminal server is a Windows Server 2003 Enterprise Edition on SP2.

Thanks,  
—Buck T.

I am guessing that the user's profile or registry are not unloading correctly when the user logs off. Microsoft makes a program just for this occasion and is used for TS servers with roaming profiles. I know you said that they stopped roaming profiles but just in case I would install "User Profile Hive Cleanup Services." You can find it with a simple Google search. I have it installed on four of our TS servers and when a user logs off it helps in cleaning up the profile and removing it after the transfer opposed to keeping an update on the server and only updating it upon login.

Also, I am familiar with ScriptLogic/Desktop Authority. It's actually a sweet piece of software and its main function is login scripts. It can make an admin's life much easier but it does have its downside. You may want to disable it for that user and see if the error returns. ScriptLogic can also do logoff scripts as well and maybe something is taking too long to run and hosing the profile in the process. Those are my thoughts, hope they help.

—John Sorensen

Network/Systems Administrator

InstantDoc ID 103635



## Deep Dive into Windows 7 Deployment, eLearning Series with John Savill

Join us on April 28 for 3 online lessons and Q&A sessions, and understand the key factors and processes to successfully deploy Windows 7 in your organization. We will explore the key functionality areas that bring business justification to the adoption of Windows 7 and the gains achieved for both the users and administrators.

Register today: [windowstipro.com/go/elearning/Windows7Deployment](http://windowstipro.com/go/elearning/Windows7Deployment)

## Why Hope Isn't a Good Enough Disaster Recovery Plan

Are you covered in the case of disaster and unplanned downtime? Too often, due to complexity and cost, we overlook a full protection strategy comprised of backup, replication, and recovery. View this on-demand seminar to learn how a solid disaster recovery plan will help you meet the strictest recovery time and recovery point objectives, and achieve instantaneous application and data recovery for central and remote locations.

[windowstipro.com/go/HopeDRStrategy](http://windowstipro.com/go/HopeDRStrategy)

## Backups . . . Do We Even Know How to Use Them?

Many companies perform basic system level backups and have never tried to actually use their backup nor understand the correct process. In this session we explore the importance of application-aware backup, which enable very granular levels of restoration but also best practices around when to backup, what to backup, how restore processes work for many different scenarios and how we should be testing them regularly.

[windowstipro.com/go/Backup101](http://windowstipro.com/go/Backup101)



Follow us on Twitter at [www.twitter.com/SavvyAsst](http://www.twitter.com/SavvyAsst)



"If you're taking part in SA, you owe it to your workplace to at least evaluate MDOP. There's some serious enterprise management muscle to be had here."

## What You Need to Know About Microsoft Desktop Optimization Pack 2009 R2

Microsoft has long espoused a "good, better, best" philosophy for its corporate customers. Sure, just upgrading a single part of your infrastructure—Windows 7 on the client, perhaps, or Windows Server 2008 R2—will give you good results. But for a better experience, the software giant recommends upgrading two infrastructure parts—the client and the server, where possible—because of the integration pieces that come into play only in such a scenario. For the vaunted "best" part of the equation, however, you'll need to consider one of Microsoft's best-kept secrets. This is the Microsoft Desktop Optimization Pack (MDOP), a diverse and useful set of utilities that should quickly become the favorites of any admin or IT pro. The latest version, the unfortunately named MDOP 2009 R2, adds a host of new features and capabilities and Windows 7 compatibility. Here's what you need to know about MDOP 2009 R2.

### What MDOP Is and How to Get It

MDOP is a set of PC management capabilities provided on a subscription basis to Microsoft customers in the Software Assurance (SA) volume licensing program. It currently consists of six core products that provide critical enterprise services such as virtual and streaming application deployment, asset inventory, advanced Group Policy change management, desktop troubleshooting and repair, and more. These diverse capabilities all have one thing in common: Each of the MDOP products helps to reduce the overall total cost of ownership (TCO) of Windows 7 desktops in an enterprise environment.

Microsoft makes broad claims about the TCO benefits of MDOP 2009 R2 and says rolling out MDOP in your environment will save from \$5 to \$125 per PC per year, depending on the tools and technologies you use. Pricing is approximately \$10 per desktop per year, depending on the type of SA subscription.

Microsoft aims MDOP at those admins and IT pros who spend time putting out fires rather than proactively improving their infrastructure. By providing desktop optimization tools that help them manage common IT tasks more efficiently, the company hopes these admins and IT pros can turn their attention and skills to tasks that will improve their businesses.

Microsoft tells me that MDOP is, by far, the most popular SA product it has ever offered. In fact, some of the tools are so good that I've pressed the company on numerous occasions to consider providing them outside of the SA program. For now, however,

MDOP remains an SA perk. Here's what's available in MDOP 2009 R2.

### Application Virtualization

One of two desktop virtualization solutions in MDOP, Application Virtualization (App-V) provides a way to stream virtualized application packages to user desktops as managed services. Because the applications being streamed are never installed directly on end-user PCs, they can be more easily managed. (Compare this to a more typical application virtualization scenario based on backwards compatibility.)

This cuts down on testing, upgrading, and compatibility issues, because the applications are isolated from native applications running locally on the PC. It can also lower software acquisition and management costs, since applications can be streamed to desktops when they are needed and easily updated on the server.

Customers who rolled out System Center Configuration Manager (SCCM) 2007 R2 or System Center Operations Manager (SCOM) 2007 can integrate these management tools with App-V via the App-V Group Policy Administrative template and App-V Management Pack. So there's no need for separate tools to deploy, manage, and track App-V-based application licenses. (Note: At press time, Microsoft announced that it would ship MDOP 2010 later this year and include new versions of App-V and MED-V that are compatible with Windows 7 and Windows Server 2008.)

### Microsoft Enterprise Desktop Virtualization

The second of MDOP's two desktop virtualization solutions, Microsoft Enterprise Desktop Virtualization (MED-V) is essentially a managed version of the Windows Virtual PC and Windows XP Mode technologies that debuted in Windows 7. It provides a way to deploy virtual machines (VMs) and bundled applications to user desktops, letting users run legacy virtualized applications seamlessly and side-by-side with native Windows 7 applications.

MED-V is all about backwards compatibility: Some legacy applications, especially custom apps and line of business (LOB) apps, simply don't run properly in newer OSs such as Windows 7, even with its improved application compatibility and troubleshooting infrastructure. In these cases, it's possible to run legacy applications in a virtualized version of Windows XP, which typically offers much better compatibility than Windows Vista or Windows 7. What



MED-V adds to this capability is application provisioning based on Active Directory Users and Groups, website redirection for sites that require Internet Explorer (IE) 6.0, and of course the ability to run legacy Windows applications side-by-side with natively compatible Windows 7 apps. If you're looking at a Windows 7 migration but have some legacy applications that simply won't run properly, MED-V is the way to go.

## Advanced Group Policy Management

Advanced Group Policy Management (AGPM) adds change management, versioning, and role-based administration control to Group Policy, providing for a more fine-grained and powerful management experience. For example, it builds on the Group Policy Object (GPO) management delegation model native to Windows by adding the ability to track, control, and review changes made to GPOs by different admins and IT pros and search for changes that were made by a particular individual or on a particular site. It also provides the ability to copy and paste GPOs from one Active Directory (AD) domain to another and filter GPOs by attributes such as name or state.

## Asset Inventory Service

Deployed as a hosted service and not as an on-premises server, Asset Inventory Service (AIS) examines the software installed on PCs and servers in your environment and helps you accurately determine whether you're in compliance with software licensing and policy. AIS is useful in many scenarios, but for those considering a Windows 7 migration, this solution is key to determining what software is in your environment so you can ensure that it's Windows 7 compatible ahead of time. (Microsoft also offers on-premises inventory capabilities in its SCCM product if you'd rather not store information about your environment on Microsoft servers.)

## Diagnostics and Recovery Toolset

Building on tools that were first made available through Mark Russinovich's Sysinternals toolset, the Diagnostics and Recovery Toolset (DaRT) provides a consistent repair and recovery environment for XP, Vista, and Windows 7 desktops and various Windows Server versions. If you're familiar with the recovery tools that come with desktop versions of Windows, you'll immediately notice that DaRT is far more powerful. It provides an offline registry editor, admin password recovery, a crash dump analyzer, file restore capabilities, advanced disk tools (including ERD Commander), secure disk erase, a host of computer management functionality (including an event viewer), a hard-drive file browser, a hot-fix uninstaller, a system file repair utility, and more.

I assume the benefits of such a full-featured tool are immediately obvious. This is a serious IT tool that would benefit admins, IT pros, and Help desk personnel in any environment.

## System Center Desktop Error Monitoring

System Center Desktop Error Monitoring (DEM) helps admins examine OS and application errors as they happen and solve PC issues proactively. Normally, this information is sent directly to

Microsoft so that the company can aggregate and evaluate issues, accelerating the response for those that are particularly widespread or dangerous. But with DEM, organizations can choose to intercept this data before it goes to Microsoft and observe issue trends that occur within their own organizations. This helps IT become more proactive about such issues.

The best aspect of DEM, perhaps, is that it doesn't require an agent installation on user desktops. Instead, this solution uses the error reporting infrastructure that's already built into Windows. All you need to do to enable DEM is toggle a GPO in AD. (Microsoft also offers a more complete and integrated error monitoring solution as part of its SCOM solution; this solution requires you to install an agent on each desktop and server to gather error monitoring information.)

## Recommendations

We're at an interesting juncture when it comes to desktop PC management. On the one hand, Microsoft is providing customers with a monster of its own making—a multifunction desktop OS with decades of improvements and backwards-compatibility capabilities that is as powerful as it is hard to manage. On the other hand, larger customers, especially those that take advantage of the software giant's SA program, have an impressive and ever-improving set of technologies they can access to improve and optimize desktop management and rein in some of Windows' less desirable traits.

Simplification is coming: I expect Microsoft to dramatically alter its desktop OS and use virtualization technologies it debuted in MDOP to remove legacy technologies from Windows. In this sense, MDOP tools like App-V and MED-V provide enterprises with capabilities that, no doubt, will become mainstream down the road.

However, people are confused about the dual desktop virtualization solutions as they now stand. The differences between the two are important: MED-V is primarily concerned with backwards compatibility; App-V is for simplifying application deployment. So while MED-V-based apps will generally run within a virtualized legacy Windows version and take on that environment's look and feel, App-V applications can run under Windows 7 and take on the Windows 7 look and feel. These are both important capabilities, but when you factor in other Microsoft virtualization capabilities, like the presentation virtualization offered by Remote Desktop Services (formerly Terminal Services), some confusion is justified.

Although I can't verify Microsoft's TCO claims, I can say that MDOP is an unparalleled collection of tools and technologies. I can quibble over whether some of these should be included in Windows proper already. But if you are taking part in SA, you owe it to your workplace to at least evaluate MDOP. There's some serious enterprise management muscle to be had here, and it comes with a minimum of overhead, learning curve, and cost.



InstantDoc ID 103602

**PAUL THURROTT** (thurrott@windowsitpro.com) is the news editor for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

# Deep Dive into Windows 7 **DEPLOYMENT** eLearning Series

with John Savill

## **WHEN**

April 28, 2010

## **WHERE**

Your computer

## **COST**

\$99

## **LESSONS**

**11:00 am ET – The Windows 7 platform**

**12:30 pm ET– Preparing for a Windows 7 Deployment and desktop upgrade**

**2:00 pm ET – Architecting the right desktop infrastructure**

## **HOW**

Register at [www.windowsitpro.com/go/elearning/Windows7Deployment](http://www.windowsitpro.com/go/elearning/Windows7Deployment)

**Get the skills and tools you need to ensure that Windows 7 is deployed and maintained in the most optimal way.**

Join expert John Savill for 3 in-depth lessons and Q&A sessions on the key factors and processes to successfully deploy Windows 7 in your organization.

## **What you'll take-away from this exclusive eLearning series:**

- Understand the different deployment technologies available
- Be able to identify the best method to document the existing desktop environment
- Estimate a timeline to deploy Windows 7
- Understand the application deployment methods and their relative advantages and disadvantages
- Develop practices to not only gather user data and personality for migration purposes but architect the optimal model for data storage going forward

## **INSTRUCTORS:**



John Savill is the director of Hitachi Consulting Services, the author of the popular *FAQ for Windows*, and a contributing editor to *Windows IT Pro*. He's an MCITP: Enterprise Administrator for Windows Server 2008 and an 11-time MVP. His latest book is *The Complete Guide to Windows Server 2008* (Addison-Wesley).

Learn more about the speaker, lessons, and  
how to reserve your seat at:

[www.windowsitpro.com/go/elearning/Windows7Deployment](http://www.windowsitpro.com/go/elearning/Windows7Deployment)

# Windows IT Pro





"Diskpart's ability to expand and shrink volumes is a welcome addition to the list of built-in Windows storage tools."

## Formatting and Resizing Partitions with Diskpart

If you've ever needed to change a volume's size, this tool is for you

In last month's "Initializing Windows Disks with Diskpart" (InstantDoc ID 103422), I showed you how Diskpart lets you view, select, create, and obtain detailed information about disk partitions. This month, we'll make those partitions useful by formatting them and giving them drive letters, then we'll see how to resize an existing partition to make it larger or smaller.

In last month's example, we added an empty 24GB drive to a Windows system and created a 10GB partition by typing *select disk 1* (which pointed Diskpart to the second physical hard disk) and *create partition primary size=10240* (Diskpart prefers size information in megabytes). To complete this disk's setup, we need to give it a drive letter with the Assign command, then format it with the Format command.

The Assign command is simple: After you focus Diskpart on a partition or volume, you can give that partition/volume a drive letter (or change the existing drive letter) by typing

```
assign [letter=<letter>]
```

To set this partition's drive letter to T, for example, you would use

```
assign letter=t
```

(If you don't specify a letter, Diskpart automatically assigns the next available letter to the partition.)

Now, you need to format the disk before you can use it. The syntax of Diskpart's Format command is a bit different from the syntax of the native Format command that Windows OSs have had since DOS 1.0. It has many options, but in most cases these options will do the trick:

```
format fs=<filesystemtype> [quick] [label=<label>]
[unit=<clustersize>]
```

For example, you could format the partition quickly, allow Format to use the default cluster size, and label it "Data drive" by typing

```
format fs=ntfs label="Data drive" quick
```

That command gives you a working disk volume, but what if you want to change the volume's size? Since Windows Vista, Diskpart has been able to expand or shrink a partition/volume. Why shrink an existing volume? I've had to do it on a number of Vista and Windows Server 2008 systems because Windows' useful BitLocker drive-encryption tool lets you encrypt entire OS drives—but only if you have the foresight to leave 1.5GB of unused space on the disk where the OS resides. Because Vista/Server 2008 Setup is sadly BitLocker-unaware (a problem that Windows 7 and Server 2008 R2

don't share), many Vista/Server 2008 users carefully set up their systems, add BitLocker as a final touch, then find that BitLocker won't work without a 1.5GB partition. Oops!

I've used Diskpart to help many people in this situation. The tool's Shrink command reduces an existing partition's size without damaging that partition. To shrink a partition/volume, I'd first select that partition or volume. For example, if I want to shrink the C drive on a system by 1.5GB, I would type *list volume* to determine the volume number that specifies the C drive (e.g., volume 2), select that volume by typing *select volume 2*, then type

```
shrink [desired=<sizeinmegabytes>] [querymax]
```

In my example, I need to clear 1,500MB of free space so that I can create the partition that will make BitLocker happy. If I just type *shrink* without any parameters, Diskpart computes the maximum space it can extract from C, then shrinks C by that amount. But I don't want C minimized in size; I just want 1,500MB taken from it. So, I'll add the *desired=* parameter:

```
shrink desired=1500
```


That command will give me the 1.5GB of space I need to set up that extra drive letter that Vista/Server 2008's BitLocker needs. To see how much space you can snatch from an existing drive, you can type *shrink querymax*.

Consider the opposite situation. You have a volume on a drive that doesn't fill that drive, leaving some precious disk space unused. How do you expand the volume to use all remaining space? You can use Diskpart's Extend command:

```
extend [size=<sizeinmegabytes>]
```

As with Shrink, first shift Diskpart's focus to the volume/partition you want to extend. Then, either type simply *extend*, which causes Diskpart to expand the volume/partition as much as possible, or constrain the extension with the *size=* parameter:

```
extend size=100
```

Diskpart's ability to expand and shrink volumes is a welcome addition to the list of built-in Windows storage tools. Next month, we'll take a look at a new-to-Windows-7 storage capability: the ability to create and manipulate drives packaged in VHD format. 

InstantDoc ID 103539

**MARK MINASI** ([www.minasi.com/gethelp](http://www.minasi.com/gethelp)) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 25 books, including *Mastering Windows Server 2008 R2* (Sybex). He writes and speaks around the world about Windows networking.

# Yet Another 10 Free Tools for System Administrators

Audit Active Directory and file servers, detect inactive users, block USB devices, and more – for free

*The following freeware tools by Windows IT Pro Community Choice Awards finalist NetWrix Corporation can save you a lot of time and make your network more efficient – at absolutely no cost. Some of these tools have advanced commercial versions with additional features, but none of them will expire and stop working when you urgently need them.*

**10. Disk Space Monitor** (MS TechNet Magazine Sep'09: [www.tinyurl.com/zksfuw](http://www.tinyurl.com/zksfuw)) — Even with today's terabyte-large hard drives, server disk space tends to run out quickly and unexpectedly. This simple monitoring tool will send you daily reports regarding all servers that are running low on disk space, below the configurable threshold. Download link: [www.tinyurl.com/dfg39kjm](http://www.tinyurl.com/dfg39kjm)

**9. Bulk Password Reset** (reviewed by SoftPedia: [www.tinyurl.com/cxc3t4d](http://www.tinyurl.com/cxc3t4d)) — While most companies have strong password policies for their employees, one critical issue is still neglected: local Administrator passwords on all servers are usually managed in a “set and forget” fashion, sometimes using some “well-known” passwords, opening a major surface for security attacks. The Bulk Password Reset tool quickly resets local account passwords on all servers at once, making them more secure. Download link: [www.tinyurl.com/kc2d9a](http://www.tinyurl.com/kc2d9a)

**8. Windows Service Monitor** (WindowsReference.com: [www.tinyurl.com/dakjw32](http://www.tinyurl.com/dakjw32)) — This very simple monitoring tool alerts you when some Windows service accidentally stops on one of your servers. The tool also detects services that fail to start at boot time, which sometimes happens, for example, with Exchange Server. Download link: [www.tinyurl.com/apfe87xl](http://www.tinyurl.com/apfe87xl)

**7. VMware Change Reporter** (TechTarget/SearchVirtualDesktop: [www.tinyurl.com/dsdz44](http://www.tinyurl.com/dsdz44)) — If you don't know what is being changed by your colleagues in the VMware infrastructure, it's very easy to get lost and miss changes that can affect the things for which you are responsible. This tool tracks and reports configuration changes in VMware Virtual Center settings and permissions. Download link: [www.tinyurl.com/qs4nv89](http://www.tinyurl.com/qs4nv89)

**6. Active Directory Object Restore Wizard** (4sysops.com: [www.tinyurl.com/kv83sh9](http://www.tinyurl.com/kv83sh9)) — This tool can save the day if someone accidentally (or intentionally) deleted a bunch of Active Directory objects. It provides granular object-level and even attribute-level restore capabilities to quickly rollback unwanted changes (e.g., mistakenly deleted users, modified group memberships, etc). Download link: [www.tinyurl.com/aspixd2](http://www.tinyurl.com/aspixd2)

**5. File Server Change Reporter** (4sysops.com: [www.tinyurl.com/bhd3k2b](http://www.tinyurl.com/bhd3k2b)) — This tool enhances the line of auditing tools; this one for file servers. File Server Change Reporter detects changes in files, folders, permissions, tracks deleted, and newly-created files, and sends daily summary reports. This is a very useful tool to detect mistakenly-deleted files and recover from backup or to see if someone changes some important files. Download link: [www.tinyurl.com/rgg821gt](http://www.tinyurl.com/rgg821gt)

**4. Inactive Users Tracker** (MS TechNet Magazine May'08: [www.tinyurl.com/xv83dsf](http://www.tinyurl.com/xv83dsf)) — This feature tracks down inactive user accounts (e.g., terminated employees) so you can easily disable them, or even remove them entirely, to eliminate potential security holes. The tool sends reports on a regular schedule, showing what accounts have been inactive for a configurable period of time (e.g., 2 months). Download link: [www.tinyurl.com/eu2kls3](http://www.tinyurl.com/eu2kls3)

**3. Password Expiration Notifier** (Redmond Magazine Feb'09, 4sysops: [www.tinyurl.com/kbwu34z](http://www.tinyurl.com/kbwu34z)) — This tool will automatically remind users to change passwords before they expire to keep you safe from password reset calls. It works nicely for users who don't log on interactively and, thus, never receive standard password change reminders at log on time (e.g., VPN and OWA users). Download: [www.tinyurl.com/4gfyrbn](http://www.tinyurl.com/4gfyrbn)

**2. USB Blocker** (Windows IT Pro Nov'09: InstantDoc ID 102860) — Users bring tons of consumer devices: flash drives, MP3 players, cell phones, etc., into the office and this aptly-named tool can block them with a couple of mouse clicks to prevent the spread of a virus and to restrict the take-out of confidential information. The product is integrated with Active Directory and is very easy to use. Download link: [www.tinyurl.com/awqc4p3](http://www.tinyurl.com/awqc4p3)

**1. Active Directory Change Reporter** (Windows IT Pro Sep'09: InstantDoc ID 102446, Windows IT Pro Jan'09: InstantDoc ID 100593, TechTarget: [www.tinyurl.com/hgfd63y](http://www.tinyurl.com/hgfd63y)) — This is a simple auditing tool to keep tabs on what's going on inside Active Directory. The tool tracks changes to users, groups, OUs, and other types of AD objects, and sends summary reports with full lists of what was changed and how it was changed. In addition, it has a nice “rollback” feature that helps rollback unwanted changes (including deletions) very quickly. Download link: [www.tinyurl.com/cph99tu](http://www.tinyurl.com/cph99tu)



"For everyone who lives in Outlook (and isn't that everyone!), one of the biggest changes in Office 2010 is Outlook's new Ribbon UI."



## New Features in Office 2010

More Ribbon, a 64-bit version, and other features will help you work more efficiently and securely

**M**icrosoft will have a banner year for new releases in 2010. Even so, one release will affect more users than any other: Microsoft Office 2010. Office enjoys near-ubiquitous status and is in use by a majority of businesses worldwide. Although previous versions of Office are tough acts to follow, Microsoft has still managed to add many significant enhancements to the Office 2010 release. Let's take a look at some of the cool new features in Office 2010.

windows, then select the screenshot of the desired window and insert it into your document.

**5 Image Background Removal tool**—A closely related feature is the new image Background Removal tool. You typically don't want to include the background of your screen captures in the images you use in your document. Previously, you needed to use another image editing tool to delete the unwanted background. The Background Removal tool lets you get rid of the background without leaving Word or PowerPoint.

**4 PowerPoint can record direct to video**—Another cool PowerPoint 2010 enhancement is the ability to record presentations directly to video. In case you were wondering, there's also basic video editing capability that lets you edit videos in PowerPoint 2010 without the need for third-party tools.

**3 Coauthoring in Word, PowerPoint, Excel, and OneNote**—I can see how Office 2010's new coauthoring feature can be a benefit to many businesses. Coauthoring lets multiple authors work simultaneously on the same document and merge together each author's work. Coauthoring requires that the shared documents are stored on SharePoint 2010.

**2 Jump lists for Outlook**—One cool feature in Outlook 2010 is the addition of the Windows 7-style jump list. You access Outlook 2010's jump list simply by hovering over the Outlook icon in the taskbar. Outlook 2010's jump list lets you quickly create new email messages, appointments, contacts, and tasks without opening Outlook and navigating through its menu options.

**1 New Ribbon UI for Outlook and OneNote**—Without a doubt, for everyone who lives in Outlook (and isn't that everyone!), one of the biggest changes in Office 2010 is Outlook's new Ribbon UI. I wasn't too crazy about the Ribbon at first, but like most things you use every day, I came to like it and was happy to see it added to Outlook. The Ribbon UI has also been added to OneNote, completing the adoption of the Ribbon across the entire Office suite.



InstantDoc ID 103593

**MICHAEL OTEY** (motey@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 New Features* (Osborne/McGraw-Hill).

**10 New native 64-bit version**—Office 2007 was available only in a 32-bit version. When you start to install Office 2010, you'll see right away that Microsoft has made a native 64-bit version of Office 2010 because you choose which version to install. The 64-bit version lets Office 2010 take full advantage of the 64-bit Windows OS.

**9 New icons and a customizable Ribbon**—Probably the first thing you'll notice about Office 2010 are the new icons for the applications. Each icon now has a large letter representing the application's name. That's a nice touch for Outlook because the old yellow Outlook icon looked a bit too much like the Windows Explorer icon. Another nice touch is the fact that the Ribbon is no longer fixed: You can customize it with your own sections and commands.

**8 Revamped Office Button**—The Office Button now presents a new smart control panel that provides information about the current document and offers many new options to better control document printing. Inexplicably, Microsoft now calls what you see when you click the Office Button the Backstage view.

**7 Protected View for downloaded documents**—For added security, Word 2010 has a new Protected View for documents opened from the Internet. Protected View essentially presents these Internet documents in read-only mode, which prevents you from running any malicious code that might have been inserted into documents.

**6 Built-in screen capture tool**—Another handy tool is the built-in screen capture, conveniently located under the Insert section of the Ribbon. You can use it from within Word 2010 or PowerPoint 2010 to capture all the currently open

■ Newest Version of VMware Player

■ Change the PowerShell Console's Colors

## READER TO READER

### Tool Time: Run VMs and More with VMware Player 3.0

VMware, a well-known player in virtualization, offers a free tool named VMware Player 3.0 for Windows and Linux PCs. VMware Player lets you not only run virtual machines (VMs) and access removable devices connected to your PC, but also create VMs, which is new to version 3.0. (This version has other new features as well, which you can read about in the VMware Player 3.0 Release Notes at [www.vmware.com/support/player30/doc/releasesnotes\\_player3.html](http://www.vmware.com/support/player30/doc/releasesnotes_player3.html).)

You can download VMware Player 3.0 from the VMware website ([www.vmware.com/products/player](http://www.vmware.com/products/player)) or the Major Geeks website ([majorgeeks.com/VMware\\_Player\\_d4891.html](http://majorgeeks.com/VMware_Player_d4891.html)). You have to identify yourself and answer a few questions to download the package from VMware but not Major Geeks. (The package is 89.5MB.) You can also download it from the CNET website. However, as of this writing, CNET has only version 2.5.2, which doesn't include the ability to create VMs.

Installing VMware Player is simple. You can find the installation instructions in the "Getting Started Guide" at [www.vmware.com/support/pubs/player\\_pubs.html](http://www.vmware.com/support/pubs/player_pubs.html). You need to reboot after installing it. Note that VMware Player 3.0 requires a minimum of 1GB of RAM in the host system to operate.

If you don't have any VMs that you want to initially test VMware Player with, I suggest that you try VMware's free Browser Appliance, which is a virtual appliance (i.e., a prebuilt software application packaged along with an OS in a VM). Browser Appliance is a Ubuntu Linux-based VM installed with Mozilla Firefox. It lets you securely browse the Internet without leaving a trace on the physical computer. This is a good VM to test drive initially as well as use later on.

You can download Browser Appliance by going to [www.vmware.com/appliances/directory/80](http://www.vmware.com/appliances/directory/80). (The download

size is 258MB.) To install it, unzip the download file on your local hard disk.

After you've installed the Browser Appliance VM, open VMware Player. In the UI, click File, as Figure 1 shows. In the File menu, note the *Download a Virtual Appliance* option. If you select this option, VMware's Virtual Appliance Marketplace web page ([www.vmware.com/appliances](http://www.vmware.com/appliances)) opens. This marketplace contains hundreds of virtual appliances, some of which are free, that you can download.

To run the Browser Appliance VM, select the *Open a Virtual Machine* option from the File menu. (Alternatively, you can click the *Open a Virtual Machine* button in the main UI.) Browse to the directory where you installed the Browser Appliance VM, highlight the Browser-Appliance.vmx file, and click the Open button. On the VMware Player virtual machine page, click Play Virtual Machine. At this point, the VM will automatically boot Ubuntu. After a few minutes, you'll see the Browser

Appliance screen in Figure 2. To use the Firefox browser, you just need to enter a web address in the field at the top of the browser and click Go.

By default, the Browser Appliance VM is configured to preserve changes (persistent mode). You can set it to revert to its original state on shutdown (autorevert mode) by editing its configuration file. VMware VMs consist of two main files: a .vmdk file (which is the VM's virtual disk) and a .vmx file (which stores the VM's configurations). The configuration file for the Browser Appliance VM is named Browser-Appliance.vmx.

You can edit Browser-Appliance.vmx using Notepad. To do so, follow these steps:

1. Open Notepad, browse to the directory where you installed the Browser Appliance VM, and open the Browser-Appliance.vmx file.
2. Add the lines in Listing 1 to the end of the file. Save the file, then close Notepad.

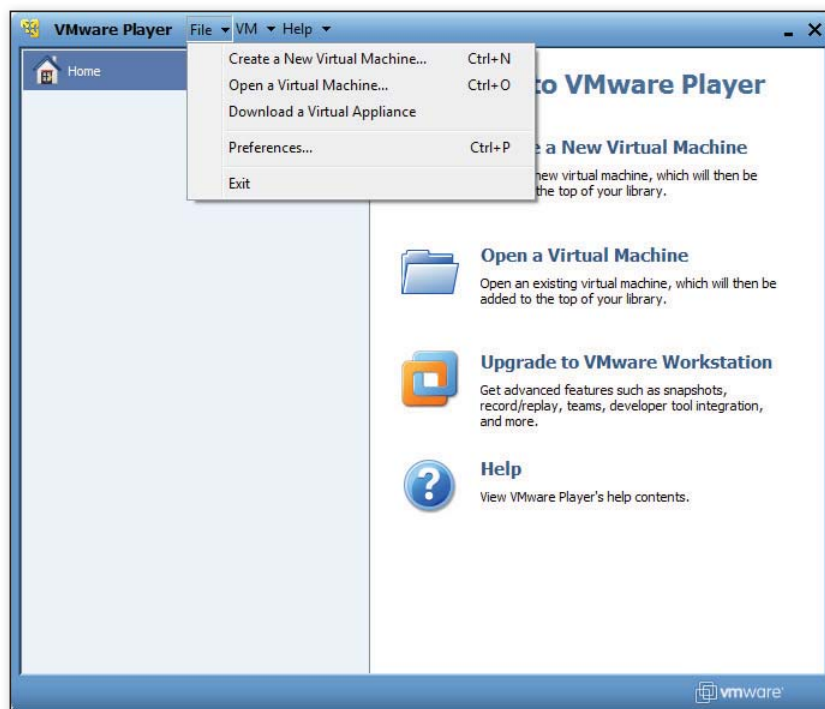


Figure 1: VMware Player 3.0's UI

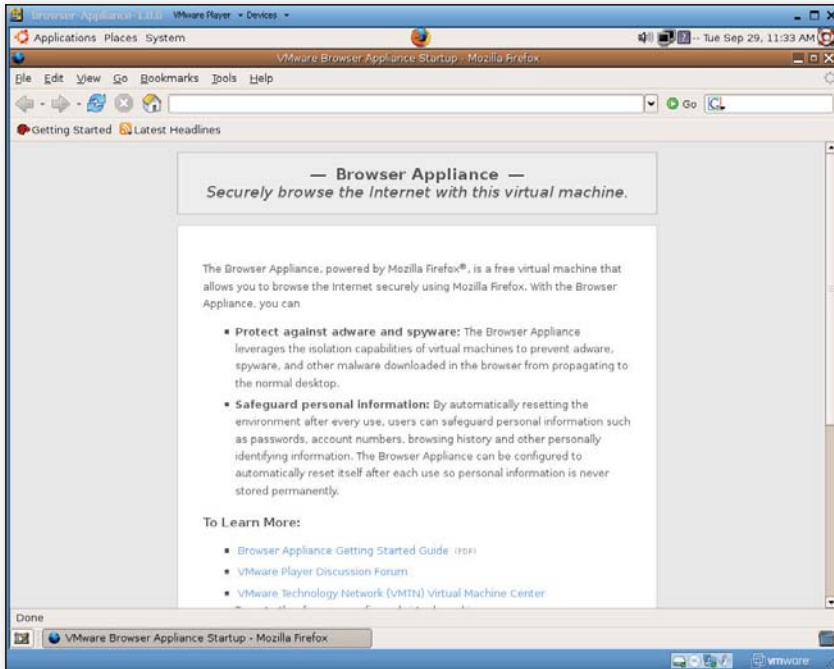


Figure 2: The Firefox browser in the Browser Appliance VM

With this configuration, all actions performed in the Firefox browser will be erased each time you shut it down. So, if you want to personalize the browser, do it before you change the Browser-Appliance.vmx file.

In VMs, you can connect to and use different types of removable devices, including DVD and CD-ROM drives, floppy drives, and network adapters.

**DVD and CD-ROM drives.** You can connect to one or more CD-ROM or DVD drives. You can also connect to disk image (ISO) files.

**Floppy drives.** You can connect to one or two floppy drives or floppy image files (e.g., .img, .flp).

**Network adapters.** You can connect to network adapters, which let you control how the VM communicates. You have three options:

- **Bridged.** The Bridged option gives the VM a virtual network that works like a real one. The VM will be able to connect to your router if you have one and receive its own IP address.
- **Network Address Translation (NAT).** The NAT option is useful if you don't have a router. The network card of

your physical machine will be used to access your network. The VM acts as if a standard network card is installed.

- **Host-Only.** The Host-Only option prevents the VM from accessing your network, but the VM will be able to connect to your physical machine. This feature is useful for testing software in a completely isolated mode.

As I mentioned previously, you can use VMware Player to create VMs. You can find instructions on how to do so in the VMware Player's Help file and on the VMware Player Documentation web page ([www.vmware.com/support/pubs/player\\_pubs.html](http://www.vmware.com/support/pubs/player_pubs.html)). You can also use third-party utilities, such as Devfarm Software's free VMX Builder ([vmxbuilder.com/vmx-builder](http://vmxbuilder.com/vmx-builder)), to create VMs.

VMware Player 3.0 is a versatile tool that's good for virtualization novices and experts alike. It's hard to believe that it's free.

—Serge Bedard,  
technology architect, CSST

InstantDoc ID 103565

## Take Control of the PowerShell Console's Colors

If you've been using PowerShell for any length of time, you might have noticed that you can control the PowerShell console's screen colors by modifying its

shortcut properties, but there aren't any cmdlets that control the console colors. Cmd.exe lets you change colors easily using the Color command, but how do you do this in PowerShell? It turns out that changing colors is pretty simple, but it requires a bit more typing than in Cmd.exe.

Cmd.exe represents colors as a pair of hexadecimal digits, where the first digit is the background color and the second digit is the foreground color (i.e., the color of the text). For example, 1F represents white text on a dark blue background. To change to that color combination in Cmd.exe, you'd use the command

Color 1F

In PowerShell, you can change the console's colors by changing the BackgroundColor and ForegroundColor properties of the \$HOST.UI.RawUI object. For example, the following pair of PowerShell commands is equivalent to the Color command just given:

```
$HOST.UI.RawUI.BackgroundColor  
= "DarkBlue"  
$HOST.UI.RawUI.ForegroundColor  
= "White"
```

(Although these commands wrap here, you'd enter each command on one line in the PowerShell console.) You can use color name strings for the Background-

Color and ForegroundColor properties because PowerShell automatically translates each string into the correct .NET type (System.ConsoleColor). Figure 3 shows the 16 possible color names and their decimal and hex equivalents. You can also use a color's numeric value instead of its name with the \$HOST.UI.RawUI object. For example, the two sample PowerShell commands can also be written as

```
$HOST.UI.RawUI.BackgroundColor = 1  
$HOST.UI.RawUI.ForegroundColor = 15
```



Bill Stewart

### Listing 1: Code to Add to Browser-Appliance.vmx

```
scsi0:0.mode = "independent-nonpersistent"  
snapshot.action = "autoRevert"  
snapshot.disabled = "TRUE"
```





Figure 3: Possible colors and their decimal and hex values

This is less verbose than using the color names, but still a lot more verbose than Cmd.exe's Color command. So, I decided to write a pair of PowerShell scripts, Get-Color.ps1 and Set-Color.ps1, which make it faster and easier to change the PowerShell console's colors.

Listing 2 shows Get-Color.ps1. When you run this script without parameters, it outputs a two-character hex string representing the current colors. The first hex digit in the string is the background color, and the second digit is the text color (i.e., foreground color). You can store the script's output in a variable, which makes it easy to restore the colors later if needed.

#### Listing 2: Get-Color.ps1

```
param([Switch] $Table)
# If -table exists, output a color list.
if ($Table) {
    for ($bg = 0; $bg -lt 0x10; $bg++) {
        for ($fg = 0; $fg -lt 0x10; $fg++) {
            Write-Host -nonewline '
                -background $bg -foreground $fg '
            (" {0:X}{1:X}" -f $bg, $fg)
        }
        Write-Host
    }
}
# Output the current colors as a string.
" {0:X}{1:X}" -f '
[Int] $HOST.UI.RawUI.BackgroundColor,
[Int] $HOST.UI.RawUI.ForegroundColor
```

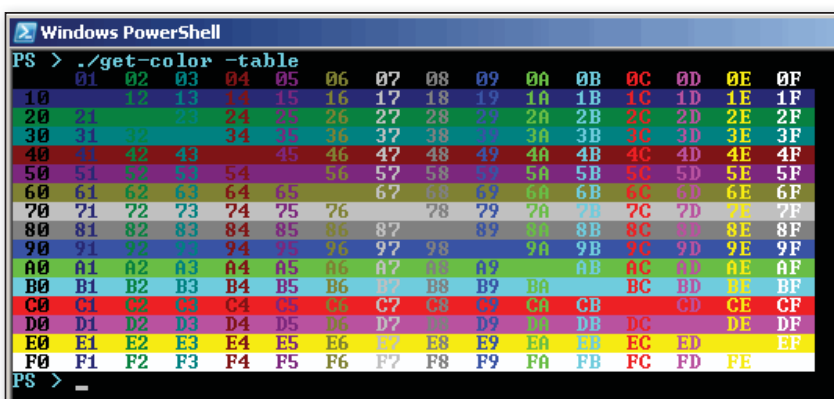


Figure 4: Possible color combinations for the console

You can run Get-Color.ps1 with the -table parameter to get a color table that displays all the color combinations (see Figure 4). You can use this table to help decide which color combination you want to use in the PowerShell console.

The Set-Color.ps1 script in Listing 3 changes the PowerShell console's colors. This script requires a single parameter: A two-digit hex value representing the new colors you want to use. Set-Color.ps1's parameter is identical to the parameter used with Cmd.exe's Color command: The first hex digit is the background color, and the second hex digit is the text color. For example, the command

```
Set-Color 9F
```

changes the console's colors to white text on a dark blue background. If the parameter you specify isn't valid or if you

set the text and background to the same color, Set-Color.ps1 generates an error.

You can combine the scripts to easily store the current screen colors, change to new colors, and restore the screen colors. For example, consider the code

```
$colors = Get-Color
Set-Color 4F
Remove-Item $ENV:Temp\* -confirm
Set-Color $colors
```

The first line retrieves the current colors using Get-Color.ps1. The second line changes the colors to white text on a dark red background (4F). The third line, which executes the Remove-Item cmdlet to delete everything in your Temp folder to free up disk space, will appear in the new colors. The last line restores the console's original colors.

#### Listing 3: Set-Color.ps1

```
param([String] $Color = '
$(throw "Please specify a color.")')
# Trap the error and exit the script if the user
# specified an invalid parameter.
trap [System.Management.Automation.RuntimeException] {
    Write-Error -errorrecord $ERROR[0]
    exit
}
# Assume -color specifies a hex value and
# cast it to a [Byte].
$Newcolor = [Byte] ("0x{0}" -f $Color)
# Split the color into background and
# foreground colors. The [Math]::Truncate method
# returns a [Double], so cast it to an [Int].
$Bg = [Int] [Math]::Truncate($Newcolor / 0x10)
$Fg = $Newcolor -band 0xF
# If the background and foreground colors match,
# throw an error; otherwise, set the colors.
if ($Bg -eq $Fg) {
    Write-Error '
    The background and foreground colors must not match.'
} else {
    $HOST.UI.RawUI.BackgroundColor = $Bg
    $HOST.UI.RawUI.ForegroundColor = $Fg
}
```

You can download Get-Color.ps1, Set-Color.ps1, and the script that created Figure 3 (EnumColors.ps1) by going to [www.windowsitpro.com](http://www.windowsitpro.com), entering 103573 in the InstantDoc ID box, clicking Go, then clicking the 103573.zip hotlink. If you're unfamiliar with how to run PowerShell scripts, see the article "Running PowerShell Scripts Is as Easy as 1-2-3," March 2010, InstantDoc ID 103427.

—Bill Stewart,  
IT systems analyst,  
French Mortuary

InstantDoc ID 103573

# Manage the Future

Desktop to Cloud

Las Vegas, Nevada | April 19-23

The Venetian Hotel

## Microsoft Management Summit 2010

The annual Microsoft Management Summit (MMS) is the premier event of the year for deep technical content on the latest IT Management solutions from Microsoft, Partner and Industry Experts.

This year's theme, **Manage the Future**, reflects the ever changing scope of IT management and the need to manage everything from device to desktop and datacenter to cloud. As initiatives such as Virtualization and Cloud Computing become widely deployed, IT Management will play an increasingly key role in reducing apparent complexity while maximizing flexibility, availability and performance.

With over 140 demo-packed technical sessions and thousands of Hands-on Lab places, MMS 2010 offers deep coverage of the latest products and solutions you'll need to "Manage the Future".

Register today at: [www.mms-2010.com](http://www.mms-2010.com)

■ Migration  
■ Outlook  
■ Clustering

■ Hyper-V  
■ DNS

## ANSWERS TO YOUR QUESTIONS

### Q: What's hard linking migration in User State Migration Toolkit (USMT) 4?

**A:** Microsoft has released an updated version of USMT that provides the features to migrate user data and state between OS instances. When migrating the information from one OS instance to another on the same machine, which is the case when a fresh OS is reinstalled on the machine, all the user state and data has to be copied to an alternate location then copied back to the machine once the new OS has been deployed.

USMT 4 introduces the hard-link migration store, which allows the user state and data to be stored locally on the computer instead of requiring storage external to the computer, and can therefore potentially save a lot of time. You use the /hardlink switch to use the hard-link migration store, and you also need to use the /nocompress option.

Hard-link migration can be used with Windows XP through Windows 7.

—John Savill

InstantDoc ID 103453

### Q: What's a Quick Part in Microsoft Outlook?

**A:** Microsoft Office Outlook 2007 introduced a new feature that, in my experience, has been quite underutilized. It's called Outlook Quick Parts, and it can improve efficiency for some users. Quick Parts are customizable, reusable content snippets for Office users. Previous versions of Outlook had a similar feature called AutoText. You can use these "building blocks," as Microsoft also calls them, as signatures, logos, text content, and more.

So why not just insert images or content when you need them instead of setting up and using a Quick Part? There are only a couple of reasons, and they may not apply to your situation. First, the Quick Part image or content is now part of Outlook. It's stored in a template. You no longer have to search outside of Outlook for it. Second, the image or content can be saved and distributed as a template for Outlook.

Quick Parts can offer benefits users for both personal and professional communication, and can help distinguish business emails from personal ones. Users create Quick Parts and they're stored locally within a Quick Parts gallery, which uses the template file NormalEmail.dotm by default. You can also choose to save Quick Parts to any other loaded template file instead.

#### Creating a Quick Part in Outlook 2007

To create a Quick Part, all you have to do is highlight the content you want to reuse and save it to the Quick Parts gallery. You do this using the Outlook email form.

### Q: I'm receiving an error about missing DLL files when adding a node to an existing Windows Server 2008 cluster. Why?

**A:** Certain cluster-aware applications register dynamic link libraries on the cluster nodes to enable specific functionality. When you add additional nodes to a cluster, a check is performed to make sure all registered DLLs exist on the new node. If any are missing, an error is shown.

The problem is that if a resource was moved to this new node of the type displayed in the warning, the required DLLs would be missing, and therefore the resource would fail to function. The solution is to make sure you install the additional software on the new node in the cluster. In my example above, I had installed a cluster-aware iSCSI target on one of the nodes prior to adding the new node.

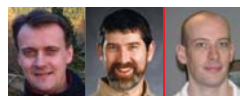
The error doesn't stop you from adding the node, and other resources that don't require the special DLLs will function with no problems.

— John Savill

InstantDoc ID 1034331

Create a new message in Outlook (or a reply or forward) and generate the content in the message body. You can type original text or cut and paste your content from another source. To form a Quick Part, you can also insert images, Smart Art, charts, hyperlinks, and just about any object that can reside in a message body. Highlight the components for the Quick Part, click the Insert tab on the Outlook Ribbon, and then click Quick Parts. At the bottom of the Quick Parts option, click Save Selection to Quick Parts Gallery. (The option won't be available if nothing is highlighted in the message body.) This opens the Create New Building Block dialog box, shown in Figure 1.

There are several options in the Create New Building Block dialog box.



Jan De Clercq | [jan.declercq@hp.com](mailto:jan.declercq@hp.com)  
William Lefkovich | [william@mojavemediagroup.com](mailto:william@mojavemediagroup.com)  
John Savill | [jsavill@windowsitpro.com](mailto:jsavill@windowsitpro.com)



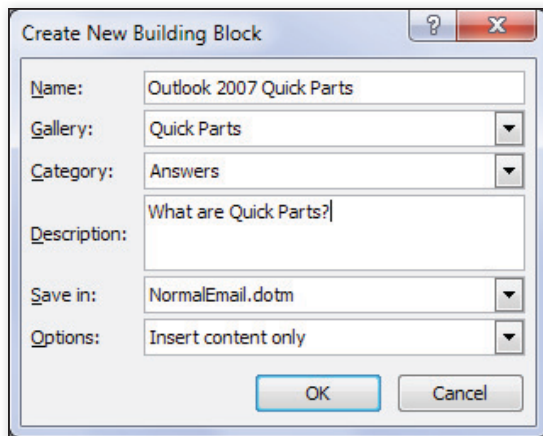


Figure 1: Create New Building Block dialog box

These options allow the user to effectively identify and reuse the content. In the first field you assign a name to the Quick Part. Outlook will assume the first few words of the text if you don't enter your own. The Gallery field can be used to sort the Quick Parts by type, but we do have categories for that and the options in the Gallery drop-down list seem more practical for Word users or email marketers. They include preset galleries of Bibliographies, Cover Pages, Headers, Footers, Watermarks, and many more. I typically use Quick Parts or the Custom Quick Parts galleries from the drop-down list.

The next field is Category, however, this does not mirror Categories elsewhere in Outlook. These are categories specifically for Quick Part organization within a Gallery. The Description field is self-explanatory and is shown when you mouse over a Quick Part in the drop-down list.

The Save In option allows you to choose which loaded template you want to store the Quick Part in. The NormalEmail.dotm template is the standard template for Outlook 2007 email composition. When you open the new email window, the message body uses the NormalEmail.dotm template. If you have any other templates loaded, then you have the option of saving the Quick Part to them. Finally, there are three options for presenting the Quick Part when it's selected for an email message: Insert content only, Insert content in its own paragraph, and Insert content in its own page. I almost always use Insert content only; however, I have some quoted content

that I saved as Insert content in its own paragraph. When you select this Quick Part, it places the text in its own paragraph, of course. It will exhibit this behavior if your cursor resides in the middle of an existing paragraph in your email. It will split that paragraph with the Quick Part. Click the OK button at the bottom to save your Quick Part. It will now display in the Insert, Quick Parts drop-down list in a new email message.

### Using Outlook 2007 Quick Parts

Applying a Quick Part to an email message is as simple as selecting Insert, Quick Parts and clicking the one you want to add. The content will appear in the message body at the cursor location. The Insert ribbon options are not available unless the cursor resides somewhere in the message body.

In the past, I had a few methods for reusing boilerplate content. When answering questions in peer forums, I kept text for common answers in separate .txt files in a folder in Windows. When a response called for one of those answers, I would open the text file in Notepad and copy and paste the content to an email reply message (or newsgroup post). I would then make any adjustments for the specific question and send. More recently, since Office 2007, I've engaged OneNote to save that content. Now, I store some of these basic replies in a template as a Quick Part and can call them from the Insert, Quick Parts tab in a new email message.

Did you know that you can save a picture as a Quick Part? Back in Outlook 2000, I saved a signature with a scanned image of my actual written signature. You can do this as a Quick Part saved with such an image. Within a new email message, select Insert Picture and locate the image to save as a Quick Part. With the image still selected or highlighted in the message, select Insert, Quick Parts to save it to the Gallery. At the end of a personal message, you can select Insert, Quick Parts and choose the signature image Quick Part.

—William Lefkovic

InstantDoc ID 103492

**Q: Do I need to upgrade to Windows Server 2008 to get Alternative Name (SAN) certificate support, or can I create a SAN certificate for my Windows Server 2003 web server using a Server 2003 Certification Authority (CA)?**

**A:** A Server 2003 CA can create SAN certificates, but it doesn't support this option by default. Before you can issue SAN certificates, you must change the configuration of the Server 2003 CA. This configuration change can only be done from the command line, with the following:

```
certutil -setreg policy\EditFlags
+EDITF_ATTRIBUTESUBJECTALTNAME2
net stop certsvc
net start certsvc
```

The last two commands stop and restart the CA service to apply the configuration change, effectively.

Next, to obtain a SAN certificate from a Server 2003 CA for your Server 2003 web server, you must use either the CA Web enrollment pages or the certreq.exe command line utility. You can't use the Certificate Request Wizard to obtain a SAN certificate on a Server 2003 system.

In the example in the question, to obtain a SAN certificate for a web server with the www.mycompany.com and the www.mycompany.net DNS namespaces using the CA Web enrollment pages, follow these steps:

1. From the web server where you want to install the SAN certificate, use a browser to connect to the CA Web enrollment pages. The default URL is `http://<CA_Server_Name>/certsrv`.
2. Click Request a certificate.
3. Click advanced certificate request.
4. Click Create and submit a request to this CA.
5. Select the Web Server certificate template and fill in the name of your web server. Most importantly, in the Additional Options section (at the bottom of the page), in the Attributes field, fill in the SAN attribute using the following syntax, as illustrated in Figure 2:

```
san=dns=www.mycompany
.com&dns=www.mycompany.net
```

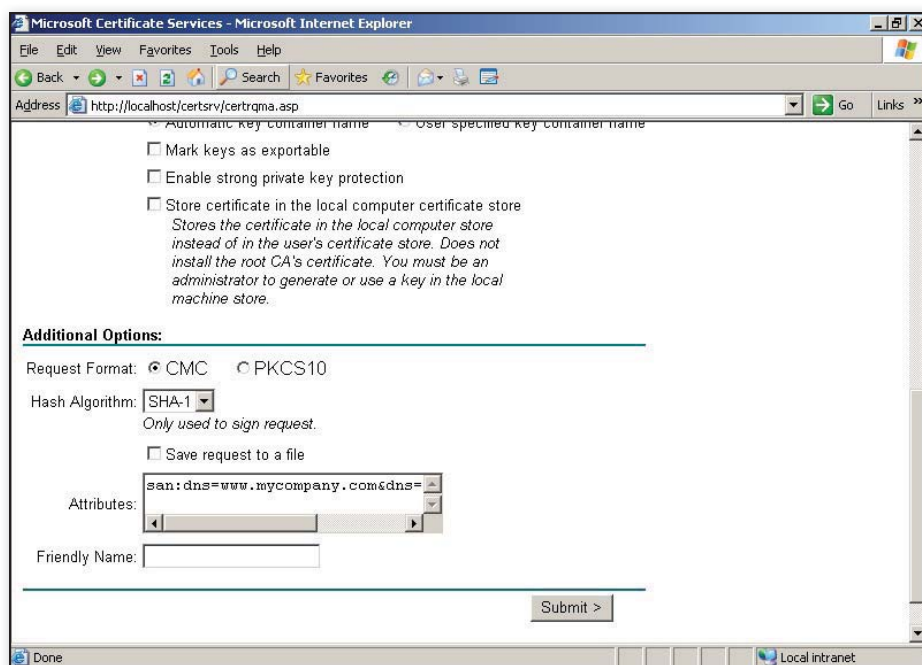


Figure 2: Additional Options for Certificate Services

6. Click Submit to send the certificate request to the CA.
7. If the certificate was generated successfully, you'll get a web page that gives you the option to install the certificate.

The Windows Server 2003 procedure for obtaining SAN certificates is outlined in greater detail in the Microsoft Knowledge Base at [bit.ly/99AIXv](http://bit.ly/99AIXv).

—Jan De Clercq  
InstantDoc ID 103403

## Q: I'm downloading some software and it has an i586 version. What's i586?

**A:** Normally, you see two types of downloads available for Windows platforms: x86 for 32-bit platform and x64 (or AMD64 or x86-64) for 64-bit.

The x in x86 means any member of the x86 family, such as 286 (16-bit), 386 (32-bit), 486, and so on, all of which were based on the Intel 8086 architecture. This list includes the 586. It was very common many years ago to hear about computers with 386 or 486 processors, but you rarely heard of 586, because the Intel 586 was actually named the Pentium (Pent for 5). The Pentium MMX processors are also 586s. The Pentium Pro, Pentium 2/3, AMD K6-2/3 are all i686, while the Pentium 4 is i786. Today's Intel i7 and AMD Phenom are the 10th generation.

If you see a version that's labeled 586, it simply means that it's built for Pentium processors or above (which really shouldn't be a problem for most of your computers).

—John Savill  
InstantDoc ID 103444

## Q: How do I enable jumbo frames within my Hyper-V virtual machines (VMs)?

**A:** Windows Server 2008 introduced jumbo frame support, but it wasn't available within Hyper-V VMs. Hyper-V 2008 R2 introduces jumbo frame support for VMs, but even with this version, the Legacy Network Adapter doesn't support Jumbo Frames.

Make sure jumbo frames are enabled on the network adapters on the Hyper-V host. Then, within the guest OS:

1. Open the Network and Sharing Center Control Panel applet.
2. Click the Change adapter settings link.
3. Right-click the network adapter and select Properties.
4. Click the Configure button for the Virtual Machine Bus Network Adapter.
5. Select the Advanced tab.
6. Select 9014 Bytes for the Jumbo Packet value.
7. Click OK.

—John Savill  
InstantDoc ID 103391

## Q: I have a zone called TrustAnchors on my Windows Server 2008 R2 DNS server. What is it?

**A:** Server 2008 R2 introduces support for DNSSEC, which allows the use of keys to ensure the integrity and source of DNS data. The TrustAnchors zone stores preconfigured public keys that are associated with a specific zone. You can view and modify these preconfigured keys by selecting Properties of the DNS server within the DNS MMC snap-in and selecting the Trust Anchors tab.

By default, the TrustAnchors zone won't exist, so if you have the zone it means someone has enabled DNSSEC in your environment and may

have configured some trust anchors. Check the content and make sure it's valid.

—John Savill  
InstantDoc ID 103516

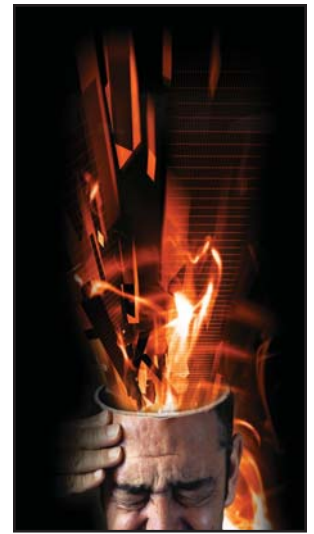
## Q: During Live Migration or vMotion migrations, I lose a couple of ping packets. Is this normal?

**A:** When using a zero downtime solution such as Hyper-V's Live Migration or VMware's vMotion, a virtual machine (VM) is moved between virtualization hosts with no downtime. In reality, there's still a slight pause of the VM as any remaining memory and device states need to be moved to the new host. Also, a reverse Address Resolution Protocol (ARP) check needs to be done to let routers know where the VM now resides. This means if you were pinging a VM as it was migrated, you may see one or two packets lost, and this is normal. The key factor is the period of unavailability is less than the TCP connection timeout value, which means that while clients may see a slight pause, they won't be disconnected from the VM that's being migrated.

—John Savill  
InstantDoc ID 103389



# Solve **4** Common Patch Management Problems



End users and your IT department can benefit from these techniques to reduce some perennial headaches

by Orin Thomas

**U**pdate management is a task IT professionals approach with the same enthusiasm they usually reserve for a visit to the dentist. Ensuring that computers are up-to-date is tedious, and at the back of every IT professional's mind is the fear that lurking somewhere deep within a newly released patch is code that will cause more problems than it solves. You need to balance thoroughly testing updates before deploying them with the knowledge that code that targets the vulnerabilities these updates address usually appears on the Internet within a week of the update's release. Spend too long pontificating on the adverse impact of applying an update and you'll become vulnerable to the exploits the update protects you against.

In this article, you'll learn about several patch-management-related problems and the steps you can take to mitigate them. The particular annoyances this article covers are as follows:

- Determining which updates have already been deployed
- Preventing update traffic from saturating WAN links
- Preventing update installations from interrupting end users' computer use
- Testing updates before deployment

This article focuses primarily on problems related to managing updates for Microsoft OSs and applications. Managing updates for third-party products without using a tool such as Microsoft System Center Configuration Manager (SCCM) 2007 poses even more challenges.

## Determine Which Updates Have Been Deployed

As more computers in organizations become mobile, administrators have more difficulty determining whether a particular update has been deployed on every computer or just on some of them. Back when I worked in first-level support, it was easy to keep track of which updates had been installed because we had to install them manually and would cross computers off a central list as each computer was updated. When updates deploy automatically over the network, it's more difficult to track whether updates have deployed successfully, unless you use solutions such as SCCM 2007.

Most organizations use Windows Server Update Services (WSUS) to manage the deployment of OS updates, as well as updates for Microsoft applications. When a configured computer contacts the WSUS server to obtain and download updates, the WSUS server records which updates computers have obtained. Computers can contact the WSUS server according to a schedule or the connection can be initiated manually. The drawback to WSUS is that although it records which updates computers have obtained, it doesn't actually check the client to see if any updates are missing, and it can be hazy on whether the update that was obtained has actually installed correctly.

WSUS knows only about updates it has provided; it has no way to know if an update has been installed in another way. For example, what if a laptop user spends a few weeks away from the office and uses Windows Update through the Internet, rather than WSUS, to keep her computer up-to-date?

## ■ PATCH MANAGEMENT

WSUS doesn't know about these updates because it's aware only of updates it distributes, not updates obtained from other locations. WSUS also knows only about computers that have reported to it. It's possible for WSUS to be completely unaware of computers on your network because, for some reason, those computers have never been able to successfully contact the WSUS server.

There are two free solutions to help with the problem of knowing which updates are installed, so you don't have to manually check each computer to see whether a specific update is installed and you don't have to deploy a solution such as SCCM 2007 that can be a drain on your IT department budget. The first free tool you can use to check computers for missing updates is the Microsoft Baseline Security Analyzer (MBSA), which you can download from Microsoft's website at [www.microsoft.com/mbsa](http://www.microsoft.com/mbsa). The latest version, MBSA 2.1.1, supports scanning Windows 7 and Windows

following script scans all computers listed in the file `computers.txt` and adds the names of computers missing the hotfix indicated by the identifier KB974332 to a text file named `Missing-KB974332.txt`:

```
get-content computers.txt | foreach
{ if (!(get-hotfix -id KB974332
-computername $_ -ea 0))
{ add-content $_
-path Missing-KB974332.txt }}}}
```

Although the code appears on multiple lines here, you would enter it all on one line. The code `-ea 0` sets the error action to silent, preventing the command from producing error text during execution.

### Prevent Update Traffic from Saturating WAN Links

Organizations deploy solutions such as WSUS not only to centralize the deployment of updates but also to minimize the amount of update traffic downloaded

server, not just those in branch offices, source their update files from Microsoft's update servers. In many organizations, the solution to this problem has been to configure separate WSUS servers at each branch office location, with branch office clients obtaining updates from their local WSUS server. However, adding WSUS servers adds to administrative overhead. It's possible to configure WSUS servers in an upstream/downstream relationship so that updates approved on one server are automatically approved on another, but every server you add to your infrastructure increases costs in some way.

The solution for branch office computers is to leverage a new technology called BranchCache in conjunction with Windows' existing Background Intelligent Transfer Service (BITS) peer caching functionality. BranchCache is a new feature for computers running Windows Server 2008 R2 and Windows 7 (Enterprise or Ultimate editions). BranchCache lets clients at branch offices share content automatically with each other when they obtain that content from an appropriately configured remote server. BITS peer caching is an existing Windows networking technology that can work in concert with BranchCache to make update transfer across the network more efficient.

You configure BITS and BranchCache through Group Policy. BITS and BranchCache policies are found in the Computer Configuration\Administrative Templates\Network node of a Group Policy Object. You can leverage BranchCache with WSUS only if the WSUS role is installed on a computer running Windows Server 2008 R2 and the client computers are running Windows 7 Enterprise or Ultimate edition.

The advantage of using BranchCache and BITS with WSUS is that organizations can use a single WSUS server to deploy updates to head office and branch office networks without saturating branch office WAN links with update traffic. Updates are retrieved across the link by one branch office client, then shared with the other clients at that location. This has the advantage of a local branch office WSUS server without the additional administrative overhead. You can find out more about BranchCache in the Microsoft article "Server

**You need to balance thoroughly testing updates before deploying them with the knowledge that code that targets the vulnerabilities these updates address usually appears on the Internet within a week of the update's release.**

Server 2008 R2 computers. You can use MBSA to check for all missing updates from a list published by Microsoft or against the list of updates that you've approved on a WSUS server. It would be nice if the MBSA tool's functionality were included with WSUS so that update deployment and checking could occur from a single console, but Microsoft currently has no plans to combine these two products.

Instead of the MBSA tool, you can use Get-Hotfix, a new cmdlet included with Windows PowerShell 2.0. Get-Hotfix lets administrators query computers locally or remotely to determine which hotfixes are installed. Using PowerShell scripting, you can query a list of computers to determine whether an update or a specific list of updates is missing. For example, the

from the Internet. Rather than 1,000 computers downloading a 100MB update, one WSUS server can download the update and then distribute it to all computers on the network. This process works fine until you take into account branch offices and saturated WAN links. Just as you generally don't want to have all your computers downloading the same large update from the Internet, you don't want to have 100 computers at a branch office all downloading the same update from the head office WSUS server across a low-bandwidth WAN link.

You can configure WSUS so that it hosts only the update approval list and not the update files, forcing WSUS clients to download update files from the Internet, but this means that all clients of this WSUS



Configuration" ([technet.microsoft.com/en-us/library/dd637785\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd637785(WS.10).aspx)).

## Prevent Updates from Interrupting End Users

When it comes to scheduling the deployment of updates, you want to avoid the scenario in which a user who has a document open leaves his computer for a short amount of time and returns to find the computer has restarted itself due to the installation of an automatic update. Users generally want their computers to restart only if they initiate the restart themselves. They really dislike computers that, from their perspective, seem to require restarts on an arbitrary basis.

I once had to spend several hours updating a manager's computer because a previous administrator had allowed the manager to choose whether to accept or reject updates after the manager had lost

requires that the computer has a BIOS that supports waking from hibernation.

If you choose this method, you should also configure policy so that the default shutdown action is to hibernate the computer rather than to power off the computer. You can accomplish this by blocking end users from being able to power off the computer, then configuring the power settings policy to automatically hibernate the computer after a reasonable period of inactivity.

## Test Updates

Every administrator fears applying the update that breaks something. It's rare today for an update to cause so many problems that it necessitates a complete OS reinstall. Most updates that fail don't do so in a spectacular and obvious manner. Failures, when they occur, are subtle. Administrators are unlikely to find a fault soon after

testers and to deploy the update to these testers a week before generally deploying the update more widely across the organization. In theory, the testers will encounter problems before the update is introduced to everyone. Inconveniencing one or two testers is less problematic than inconveniencing everyone. If testers can't find a problem in a week's worth of typical computer use, any problems that the update causes probably won't be serious.

The main difficulty in recruiting testers is that testers need only one bad experience and they might be unwilling to test anymore: Someone who loses a day's work is less likely to volunteer to be a guinea pig in future. Users in the IT department don't make good testers because they rarely use applications in the same way that other employees in the organization do. When assembling a test group, you might need to find a way to reward the users, which probably requires the support of your management. Explain to management why you need a group of reliable testers but that also, from time to time, these testers will lose working time because of something unforeseen happening because of updates on their computers. Better, though, that a small number of users lose time than the whole organization suffers downtime because an update that causes a problem gets deployed to everyone without undergoing any local testing.

**Better that a small number of users lose time than the whole organization suffers downtime because an update that causes a problem gets deployed to everyone without undergoing any local testing.**

several hours' work due to an unexpected restart caused by the installation of an automatically scheduled update. Needless to say, the manager had declined all future updates, so the computer was several service packs behind where it should have been at that point in time!


Some of the randomness of update installation can be mitigated through configuring update-related Group Policies. The *Enabling Windows Update Power Management to automatically wake up the system to install scheduled updates* policy, in conjunction with the Configure Automatic Updates policy, lets administrators configure computers to wake from hibernation at a preconfigured time to install updates. This method lets computers wake themselves for update installation at 3:00 A.M., for example, when no sane user should have a document open. This method

installing the update on a test computer. People who use the OS or applications in day-to-day situations are more likely to find faults than those who only have a passing familiarity with them.

This situation makes it difficult for administrators to know whether deploying an update will cause a problem. Just because a problem isn't immediately obvious doesn't mean it isn't serious. Vendors have released updates that caused data corruption that wasn't apparent to administrators through typical testing, but end users discovered the trouble two days after the update was rolled out to every computer in the organization.

Administrators need a way for typical end users to test updates without deploying the update to every user in the organization. One solution is to have a group of typical users that function as update

## Acceptance Is the Key

The main way to reduce the annoyance of the patch-management process is to accept that it will always be necessary and that the best way to deal with it is by being organized. Although patch management will never be something that IT professionals eagerly anticipate, following the advice in this article can reduce these specific annoyances to minor irritations. 

InstantDoc ID 103599



### Orin Thomas

([orin@windowsitpro.com](mailto:orin@windowsitpro.com)) is a contributing editor for *Windows IT Pro* and a Windows Security MVP. He has authored or coauthored more than a dozen books for Microsoft Press.

# Prime Your Mind

with Resources from Left-Brain.com

Left-Brain.com is the online superstore stocked with educational, training, and career-development materials focused on meeting the needs of IT professionals like you.



## Featured Product:

### VMware vSphere Training

VMware vSphere Training courseware is appropriate for both new VMware administrators and those who are preparing for the VCP certification. Besides completely covering how to administer a VMware infrastructure, this course also reviews third-party solutions that are widely used by the virtualization community. Find out more about this course and other virtualization resources at Left-Brain.com

[windowsitpro.com/go/left-brain/vsphere](http://windowsitpro.com/go/left-brain/vsphere)

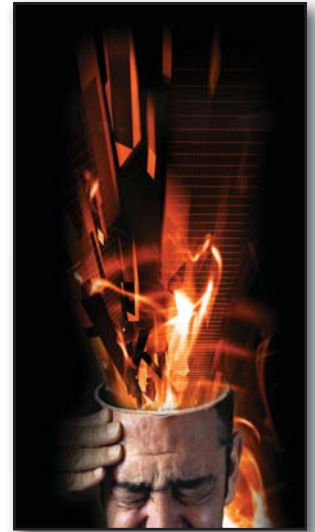


\*Plus shipping and applicable tax.

[www.left-brain.com](http://www.left-brain.com)

WindowsITPro

# 9 Workarounds for Windows 7 Woes



**A**fter the poor reception of Windows Vista by customers, Microsoft knew it had to retrench for that system's successor, Windows 7. And retrench it did. Windows 7 has entered the market to universally positive reviews from the tech press and customers alike. One reason for the good reviews is that Windows 7 is a more modest upgrade. Another reason is that Windows 7 is a more cohesive and simpler system compared to its predecessor.

So, there's no doubt that Windows 7 is a huge success. But if you're coming to Windows 7 from a previous Windows version, you're going to notice a number of changes—some big, some small. And while Windows 7's changes are mostly improvements, unfamiliarity can lead to a loss of productivity. So, if you're looking for a way to fix some of Windows 7's most obvious annoyances or to change some crucial feature back to the way it used to work, fear not: We've got your back.

## Taskbar

When you look at Windows 7's UI, the most obvious change is the new taskbar, which represents a major functional departure from previous Windows versions. Instead of just providing buttons that represent running applications and other open windows, the taskbar also commingles shortcuts for frequently needed applications and other objects. If you're familiar with Mac OS X, you might feel that the new taskbar is a rip-off of that system's Dock. In many ways, however, it simply combines the functionality of the Vista and XP taskbars with the Quick Launch toolbar. Regardless of its origins, one thing is clear: The Windows 7 taskbar is different enough that it will cause some headaches for users who are accustomed to previous Windows versions.

**Annoyance:** By default, the Windows 7 taskbar displays only a single icon for every shortcut or button, as Figure 1 shows. So, if you have several Internet Explorer (IE) windows or tabs open, you'll see only one button. That can be confusing. It also means that there's no descriptive caption on the button to describe what the windows are displaying, as was the case with all previous Windows versions dating back to Windows 95.

**Workaround:** You can overcome Microsoft's less-than-ideal default taskbar behavior and arrive at a display that more closely resembles previous Windows versions. To do so, right-click a blank area of the taskbar and choose Properties. Then, in the Buttons drop-down list on the Taskbar tab, choose *Combine when taskbar is full*. This will cause the taskbar to make two display changes. First,



Figure 1: The default taskbar

How to deal with the new OS's taskbar, compatibility issues, and more

by Paul Thurrott





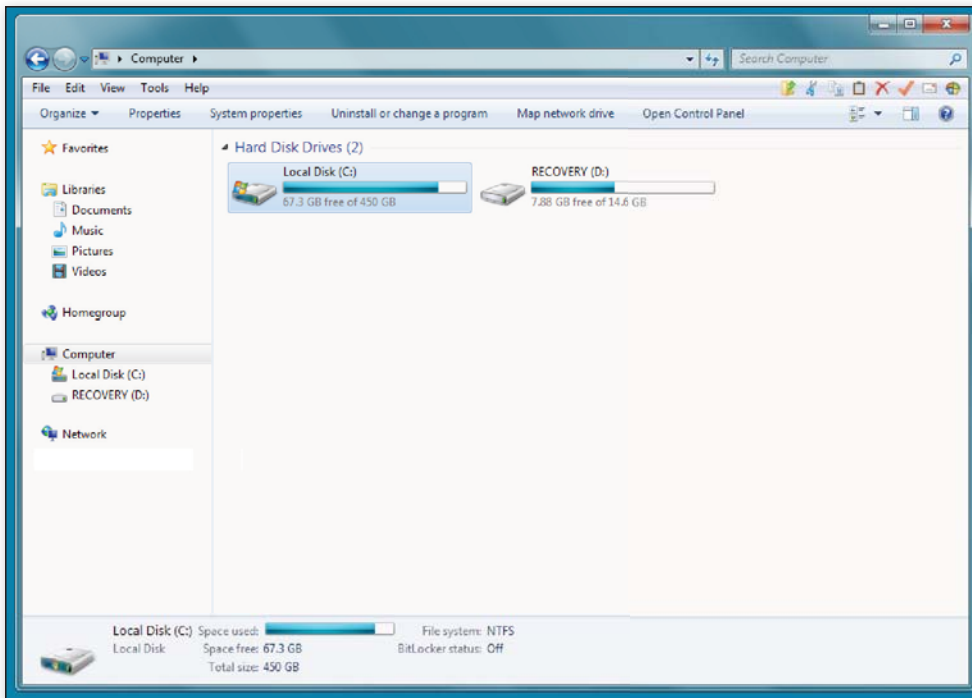


Figure 4: Classic Shell's mini toolbar in Windows Explorer

applications into believing that they're running under older Windows versions. Unlike previous versions, Windows 7 has a new troubleshooting infrastructure that provides wizards for compatibility issues and a host of other common problems. These wizards provide step-by-step walk-throughs in plain English, making it much easier to work through problems.

If you installed a program that isn't working and you want to easily determine whether it can be made to run correctly under Windows 7, type *action* in the Start menu's Search box, open the Action Center, and click the Troubleshooting link. Under Programs, click *Run programs made for previous versions of Windows* to bring up the Program Compatibility wizard. (Alternatively, you can run this wizard by typing *compat* into the Start menu's Search box.) The Program Compatibility wizard will then walk you through the steps needed to address the compatibility problem.

**Annoyance:** An application still won't install or run under Windows 7.

**Workaround:** Some legacy applications simply won't install or run correctly under Windows 7. In this case, new features called Windows Virtual PC and Windows XP Mode can help you solve the problem using virtualization technology.

Windows Virtual PC is the next generation of Microsoft Virtual PC. It offers some important benefits over its predecessor, including USB support and the ability to run virtualized (i.e., guest) applications alongside native (i.e., host) applications. Windows Virtual PC is available for free to all Windows 7 users, but it requires hardware virtualization support in the PC's microprocessor and BIOS.

Windows XP Mode is a specially packaged, virtualized version of XP SP3. It's free to the users of the Windows 7 Professional, Enterprise, and Ultimate editions. Because it runs under Windows Virtual PC, any applications you install inside this environment can run alongside your normal Windows 7 applications. It's the perfect solution for those few remaining applications that simply won't run in Windows 7 natively. (Note that Windows XP Mode won't work for many games and other graphically demanding applications.)

## Windows Update

Microsoft has done a nice job of improving the Windows Update application in Windows 7, but at least one glaring issue remains.

**Annoyance:** If you leave your PC unattended overnight and the system

automatically installs critical or important security updates that require a reboot, Windows Update automatically reboots your PC. So, in the morning, you might discover that all your applications have shut down and you've lost some data.

**Workaround:** You can prevent Windows Update from automatically rebooting your PC, although it will require a bit of work because the registry key that controls this functionality is missing from Windows 7. To stop automatic rebooting, open the registry editor (type *regedit* in the Start menu's Search box) and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\`

`Policies\Microsoft\Windows`. Create a new key named *WindowsUpdate*. Inside that key, create a new subkey named *AU*. In the subkey, add a DWORD (32-bit) entry named *NoAutoRebootWithLoggedOnUsers*. Set its value to 1. You'll have to restart the computer for the change to take effect.

## The Least Annoying Upgrade

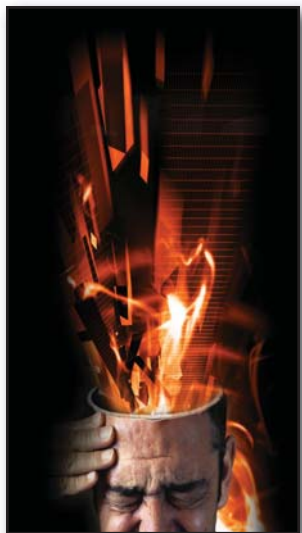
Every version of Windows comes with new challenges and new ways of doing things. Windows 7 represents a major functional improvement over its predecessor, but it's different enough from Vista and XP to cause a bit of grief. Fortunately, there are simple workarounds to most problems. While any change can be traumatic, Windows 7 is, in many ways, the least annoying upgrade Microsoft has ever shipped.

InstantDoc ID 103546



### Paul Thurrott

(thurrott@windowsitpro.com) is the news editor for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* ([www.windowsitpro.com/email](http://www.windowsitpro.com/email)) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* ([www.wininformant.com](http://www.wininformant.com)).



# Soothe **5** **ACTIVE DIRECTORY** Headaches

Some problems  
require  
upgrading,  
but some  
you can work  
around

by Sean Deuby

It's hard to believe that Active Directory (AD) has been around for ten years. AD was a revolutionary product compared with Windows NT, and over the years it has only gotten better. However, AD isn't perfect—it has its share of annoyances. In this article, I outline a few things that especially bug me about AD, including steps Microsoft has taken to improve the problems. I also suggest workarounds for those problems that are still on the “to-do” whiteboard at Microsoft's Red West campus.

## AD vs. DC Administration

A basic annoyance that's been around since Windows 2000 Server is the lack of separation between administering an AD domain or forest and administering the domain controllers (DCs) that support it. In other words, you must be a domain administrator to be able to fully administer DCs. Microsoft's position is that if you have administrative access to a DC, you should also have admin rights in the domain, because that access lets you hack the DC and elevate your privileges. Computer operators have physical access to DCs, so they can theoretically gain access whenever they want. The counter argument is strictly practical: A computer operator's job is to administer servers in the data center, and a DC should be no exception. It's impractical to say that operators should have admin rights on a machine simply because they have physical access to it; basic security practices dictate that you limit the number of domain administrators to an absolute minimum—which therefore excludes many of your computer operators.

Two workarounds let you circumvent this annoyance. The first workaround is to grant your computer operator security groups only the appropriate rights for their specific job requirements. Actions that can't be delegated (i.e., those actions that require administrative rights and that can affect AD health) must be performed by domain administrators. The Microsoft document “Best Practices for Delegating Active Directory Administration” (<http://bit.ly/5ByrEy>) details an organized plan to delegate AD service management.

The second method is to upgrade to Windows Server 2008 R2 and use read-only domain controllers (RODCs) wherever possible. An RODC is a DC configuration in which a read-only copy of AD is kept locally, and password secrets aren't kept at all. A lesser-known feature of the RODC is its administrator role separation: Unlike full DCs, administrative tasks for the RODCs can be delegated to individuals or groups without compromising the entire forest's security. The reason you can safely grant administrator rights to an RODC but not to a full DC is that, unlike full DCs, RODCs aren't trusted by the rest of the forest. RODCs never replicate changes into the forest; they only receive them. Unless you explicitly configure the password replication policy on an RODC's computer object, passwords are never stored on the RODC. As a result, granting an operator Administrator rights on an RODC doesn't compromise the forest's security. The TechNet article “Administrator Role Separation” (<http://bit.ly/4Qlffs>) describes how to enable administrator role separation on your RODCs; the “Read-Only Domain Controller Planning and Deployment Guide” (<http://bit.ly/2lGULi>) will help guide you through placing RODCs in your enterprise. For more information about Server 2008 RODCs,



see “Fortify Remote-Server Security,” [www.windowsitpro.com](http://www.windowsitpro.com), InstantDoc ID 97962.

## Service Account Passwords

One of the longest-running AD annoyances is that of service account passwords. A service account is a user object that’s dedicated to running a server service, such as Microsoft SQL Server. As for any user object, good security practices dictate that the password is changed on a regular basis. The problem is that service account passwords are hard-coded into the service’s properties; changing the account’s password without also changing it at the service location and restarting the service will cause authentication service restart problems. Interfering with a production application’s availability to simply change a password isn’t a popular IT practice. This difficulty has been around since Windows NT, which means longer than 15 years.

Server 2008 R2 solves this issue once and for all with a new feature called managed service accounts. MSAs are special accounts that automatically update their passwords and simultaneously change the password for the service on the managed computer. (For more information about MSAs and how to use them, see “Use MSAs to Ease the Pain of Administering Service Accounts,” February 2010, InstantDoc ID 103265.) The good news is that MSAs don’t require Server 2008 R2 DCs; you only need to run the `adprep /forestprep` command to upgrade the forest’s schema to Server 2008 R2. The bad news is that a server must be running Server 2008 R2 to use an MSA.

IT budgets are tight, but remedying this old annoyance is important for security. In fact, it’s a great argument for upgrading to Server 2008 R2.

## Site Subnet Configuration

I confess that IP subnet configuration has never been one of my strongest skills. I didn’t really enjoy the TCP/IP networking classes, and getting the custom subnet masks just right for the range of IP addresses I needed for an AD site always took me longer than the other kids. Inexplicably, Server 2008 R2 and Server 2008 make the task even harder than before by requiring that you enter the subnet range using network prefix notation (e.g., 192.168.1.0/20). I knew early on that I wasn’t destined to be a network

engineer—but maintaining the list of IP subnets that define an AD site is one of the standard skills an AD admin must have. Fortunately, I discovered several websites that provide IP subnet calculators to do the heavy lifting for you.

The IP Subnet Mask Calculator at [www.subnet-calculator.com](http://www.subnet-calculator.com) works well. If you want a freeware app that you can download to your client, try WildPackets’ IP Subnet Calculator, available at [www.wildpackets.com/resources/free\\_utilities/ipsubnetcalc](http://www.wildpackets.com/resources/free_utilities/ipsubnetcalc). These applications let you perform what-if scenarios to choose a custom subnet mask or network prefix that covers the IP address range you need it to, and nothing more.

## Rebuilding an Active Directory DC

Sometimes a DC’s just gotta go. It isn’t working properly, and you’ve tried everything you can think of to fix the problem, with no success. You’ve run out of time and patience, and you’ve decided that the best solution is to demote the DC—but it’s broken enough that it won’t demote. The only thing left to do is rebuild the box from scratch, do a metadata cleanup, and repromote the machine.

However, if you’re sure the DC’s OS is functioning properly and the problem is with its AD role, you can avoid the annoying rebuild task by using the `dcpromo /forceremove` command. This little-known option forcibly removes AD from the server but leaves the server OS intact. You’ll still have to do the metadata cleanup, but you’ll reduce the length of the outage because you won’t have to reinstall the OS. After the forced removal is complete and you’ve performed the metadata cleanup, you can repromote the server to a DC.

## Metadata Cleanup

To get a failed DC back into service as soon as possible, you should perform the metadata cleanup during the forced removal and reboot. A metadata cleanup is the process of manually removing information about a failed DC (i.e., its metadata) from AD that the `dcpromo` process would otherwise remove automatically. Performing a metadata cleanup is an annoyance in itself, because you have to work through `Ntdsutil` commands, on a DC, using a series of commands that aren’t obvious. Fortunately, a couple of Microsoft employees wrote a

script that removes AD DC metadata that’s left behind after the `dcpromo /forceremove` command is used. Their GUI Metadata Cleanup Utility is available in the TechNet Script Center Repository at <http://bit.ly/byByot>. This script doesn’t work with Server 2008 R2, but it doesn’t need to.

The most recent versions of Windows Server make metadata cleanup much easier than in the past. Starting with Server 2008, you can perform a metadata cleanup with a click of your mouse. Launch the Microsoft Management Console (MMC) Active Directory Sites and Services snap-in (`dssite.msc`), open the site that contains the failed DC (the default site is logically named `Default-First-Site-Name`), expand the Servers container, select the DC to be removed, then right-click and delete it. In Windows 2000, Windows Server 2003, and Windows 2003’s various service packs, deleting a DC’s computer object will generate various warnings to remind you that a metadata cleanup must still be performed. In Server 2008 R2 and Server 2008, the delete action also performs a metadata cleanup. Although this improvement isn’t enough to justify an upgrade, it’s a nice fringe benefit.

## Upgrade or Outsmart

Like any large and complicated software product, AD has its share of annoyances. The Microsoft Directory Services team is aware of all these issues and is working on solutions for them. The challenge is in refining AD and making it easier to use, while staying within the boundaries of the design and balancing the amount of time and resources necessary to make changes. Because you can’t retrofit new functionality into an existing OS, in some cases you’ll have to upgrade to take advantage of certain solutions. But sometimes, having the right knowledge lets you work around AD’s problems.



InstantDoc ID 103576



### Sean Deuby

([sdeuby@windowsitpro.com](mailto:sdeuby@windowsitpro.com)) is a contributing editor for *Windows IT Pro*, an enterprise solutions strategist with Advaiya, and former technical lead of Intel’s core directory services team. He’s been a directory services MVP since 2004.

# GIVE YOURSELF A HIGH 5

with the new benefits of a Windows IT Pro VIP membership

Become a VIP member today to boost yourself ahead of the curve tomorrow!

1

**NEW!** Free Downloadable Pocket Guides—each eBook a \$15 value!

- Business Intelligence
- Configuring and Troubleshooting DNS
- Data Warehousing
- Group Policy
- Integrating Outlook & SharePoint
- Outlook Tips & Techniques
- PowerShell 101

2

**NEW!** Free Archived On-Demand eLearning Events—each event a \$79 value! Coverage includes Exchange, SharePoint, PowerShell, SQL Server, and more!

3

1 year of VIP access to online solution database – with every article ever printed in Windows IT Pro and SQL Server Magazine, PLUS bonus web content posted every day on hot topics like Security, Exchange, Scripting, SharePoint, and more!

4

A 12-month print subscription to Windows IT Pro, the leading independent voice in the IT industry

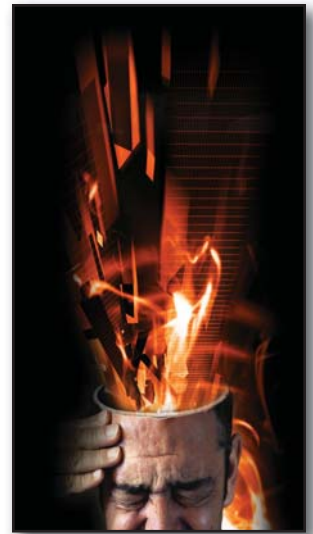
5

VIP CD with over 25,000 solution-packed articles (updated and delivered 2x a year)



Give yourself a HIGH 5 for only \$199 at [windowsitpro.com/go/High5VIP](http://windowsitpro.com/go/High5VIP)

# Prepare Now For 7 Hyper-V Migration Idiosyncrasies



Understand the  
product before  
you virtualize

by Alan Sugano

**T**he big news with the release of Microsoft Hyper-V Server 2008 R2 is Live Migration. Live Migration lets you move a Hyper-V guest from one clustered Hyper-V host to another clustered Hyper-V host while the guest is still running. This migration takes place usually within two seconds. The Cluster Shared Volumes (CSV) feature facilitates Live Migration in Hyper-V Server 2008 R2. CSV tracks which hosts are accessing which .vhd files on the SAN, allowing multiple hosts to simultaneously access a given SAN LUN. But moving to Hyper-V isn't without its problems. Being aware of these migration requirements should simplify your transition to Hyper-V from dedicated physical servers.

## Hardware Requirements

Hyper-V uses a 64-bit hypervisor kernel. Your Hyper-V host must support hardware virtualization in both the CPU and BIOS. To get this support, you'll need one of the following processors: AMD Athlon 64 (revision D or later), AMD Opteron (revision E or later), AMD Turion 64 (revision E or later), AMD Sempron 64-bit capable version (revision D or later, experimental support), or Intel EM64T VT-capable processor (experimental support).

Most middle- to high-end servers now support hardware virtualization. But if you were planning to run Hyper-V on an older server, you'll probably need to purchase new hardware. Hardware virtualization support is usually disabled on the server when it comes from the manufacturer. You enable hardware virtualization support in the computer's BIOS settings, usually in the Advanced Settings section, and it requires a hard reboot to make the setting active. Make sure you also enable the Execute Disable Bit (Intel) or NX Bit (AMD) in the BIOS to run Hyper-V.

## Memory Requirements

Like being too rich or too thin, you can never have too much memory capacity on your Hyper-V host. I suggest purchasing a server that has at least 128GB of potential memory capacity. You might not initially install the maximum amount of memory in the Hyper-V host, but it's always good to have some breathing room, especially if you plan to run Microsoft Exchange Server or Microsoft SQL Server on your Hyper-V host. Often, you can increase the performance of disk-bound x64 Windows guests by allocating more memory to the guest for disk caching. I've found that a simple Exchange 2007 server with the roles of Mailbox, Client Access, and Hub Transport, and the management tools requires about 16GB of memory to avoid memory page swapping. Plan accordingly. With the current generation of servers that use DDR3 memory, purchase DIMMs in multiples of three in the same density for the best performance.

## Hyper-V on Server Core

For the sake of security, I strongly suggest installing Hyper-V on Server Core and not the full installation of Server 2008 R2. Server Core has a significantly smaller footprint than the full version of Server 2008 R2 and requires fewer patches. You should place Hyper-V management computers on an isolated network that's separate from virtual server guest traffic. Consider placing a firewall between this Hyper-V management network and a secondary authentication device for the best security. It's important to protect the Hyper-V host because a compromise of the Hyper-V host will lead to really bad things—such as the ability to set up rogue virtual guests that can potentially hop from host to host in a clustered Hyper-V environment.



## ■ HYPER-V MIGRATION

### Management Options for Hyper-V

Installing Hyper-V on Server Core complicates management of the Hyper-V host because it must be managed from another computer. Your management options are as follows:

**Windows Server 2008 Hyper-V Tools feature.** You can install the Hyper-V Manager on Server 2008 by accessing Server Manager, Features, Remote Server Administration Tools, Remote Administration Tools, Hyper-V Tools.

**Windows Vista.** You can download and install the Hyper-V Manager for Vista. The different versions are available at

- Vista x86: [www.microsoft.com/downloads/details.aspx?FamilyId=A46D0047-E383-4688-9449-83373226126A](http://www.microsoft.com/downloads/details.aspx?FamilyId=A46D0047-E383-4688-9449-83373226126A)
- Vista x64: [www.microsoft.com/downloads/details.aspx?FamilyId=F10E848F-289C-4E04-8786-395371F083BF](http://www.microsoft.com/downloads/details.aspx?FamilyId=F10E848F-289C-4E04-8786-395371F083BF)

**Windows 7.** You must install and configure the Remote Server Administration Tools for Windows 7, available at [www.microsoft.com/downloads/details.aspx?FamilyID=7d2f6ad7-656b-4313-a005-4e344e43997d](http://www.microsoft.com/downloads/details.aspx?FamilyID=7d2f6ad7-656b-4313-a005-4e344e43997d). These tools run only on Enterprise, Professional, and Ultimate versions of Windows 7. After you install the tools, open the Control Panel Programs and Features applet and select *Turn Windows Features on or off*. Expand Remote Server Administration Tools, Role Administration Tools, Hyper-V Tools, and select the Hyper-V Management Tool.

**System Center Virtual Machine Manager (VMM) 2008 R2.** Although you can perform basic management tasks with the previous tools, if you plan to place the Hyper-V host into a production environment, I strongly suggest you purchase VMM. It's roughly \$870. It can store virtual machine (VM) templates in libraries, queue and troubleshoot live migrations, assign granular management roles, perform compatibility host checks for live migration, and has other features that you need for a Hyper-V production environment. VMM requires an x64 Server 2008 server. Although you can set up the server as a VM, the disaster recovery process will be simplified if this management server is installed on a physical machine. VMM also requires SQL Server. You can use SQL Server Express Edition, but the database size is limited to 4GB. If you want to manage more than 150 Hyper-V hosts with VMM,

you'll probably need the full version of SQL Server 2008 or SQL Server 2005.

### CPU Compatibility

Live Migration lets you move a virtual server guest from one Hyper-V host in a Hyper-V cluster without any downtime. This allows you to perform Hyper-V host maintenance during the day without having to take down any virtual servers. Just move all the virtual server guests off of a Hyper-V host before taking it down.

In an ideal environment, all the Hyper-V hosts in the cluster should be identical to guarantee the best Live Migration compatibility. There's no Live Migration between AMD and Intel Hyper-V hosts. Theoretically, you can migrate virtual server guests among Hyper-V hosts that are in the same processor family, or you can enable processor compatibility mode to increase the compatibility between hosts for Live Migration. Although the matrix shown at [vmetc.com/wp-content/uploads/2008/06/vmotion-compatibility-by-processor-from-dell.png](http://vmetc.com/wp-content/uploads/2008/06/vmotion-compatibility-by-processor-from-dell.png) refers to VMware's VMotion, it gives you the general idea of what processor families are compatible for a Live Migration move. For more information on processor compatibility mode on Hyper-V, refer to "Virtual Machine processor compatibility mode" at [download.microsoft.com/download/F/2/1/F2146213-4AC0-4C50-B69A-12428FF0B077/VM%20processor%20compatibility%20mode.doc](http://download.microsoft.com/download/F/2/1/F2146213-4AC0-4C50-B69A-12428FF0B077/VM%20processor%20compatibility%20mode.doc).

### Backup Options

For any production Hyper-V environment, I suggest obtaining .vhd image backups of the virtual server guests. These image backups greatly simplify the disaster recovery process. You don't have to worry about reinstalling any applications in the virtual server guests. Some backup options even let you perform granular restores from the .vhd images, although typically these backup images have to be stored on disk (not tape) to perform a granular restore. If you plan to use this method, make sure you have adequate disk space for your .vhd images. Even though these backups are initially stored to disk, you should still eventually copy them to some type of offline media, such as tape.

The blog "Hyper-V HowTo: Backup" at [blogs.technet.com/tonyso/archive/2009/05/26/hyper-v-how-to-backup.aspx](http://blogs.technet.com/tonyso/archive/2009/05/26/hyper-v-how-to-backup.aspx) lists some of the backup options available with Hyper-V.

If you've ever had to recover a DC, or a SQL Server or Exchange Server installation from scratch, you know that the process is stressful, complicated, and time consuming. If you have a backup of the .vhd disk images for the failed server, you can simply restore these images and start the machine. If your .vhd image backup doesn't contain the latest data backup, you might have to perform a data-only restore to your virtual server guest, but having the .vhd images greatly simplifies the recovery process.

### P2V Server Migrations

There are quite a few tools that let you migrate from a physical server to a virtual server. In general, these tools work fairly well; however, the migrated machine will be only as stable as the original physical server. If the server has been in service for any length of time, I suggest you rebuild the server from scratch from a Hyper-V Virtual Server Guest template and just migrate the data. This is similar to the situation of upgrading a workstation from Vista to Windows 7. Most IT professionals agree that the migrated workstation will be more stable if you wipe the hard drive and perform a clean install of Windows 7, rather than performing an in-place upgrade. The same rules apply to a virtual environment, except the exposure is significantly greater because you're dealing with a server, not a workstation.

If you have the luxury of building the server from scratch in a virtual environment, take the extra time to do so. The server will be more stable, and you'll have fewer problems in the future.

### Ready for Production

The Live Migration feature in Hyper-V Server 2008 R2 has positioned Hyper-V as a production-ready virtualization platform. As with any newer technology, avoiding potential pitfalls will ensure a successful Hyper-V implementation. I hope this article helps you understand those concerns and avoid any problems.



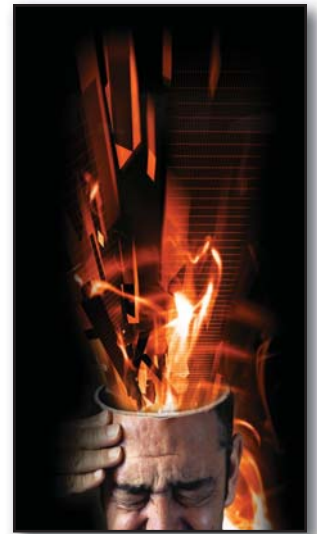
InstantDoc ID 103549



#### Alan Sugano

([asugano@adscon.com](mailto:asugano@adscon.com)) is the president of ADS Consulting Group, which specializes in networking, custom programming, Microsoft .NET web development, and SQL Server development. He's the author of *The Real-World Network Troubleshooting Manual* (Charles River Media).

# 4 Failover Clustering Hassles and How to Avoid Them



Take another look at failover clustering—its old reputation doesn't apply

by John Savill

**F**ailover clustering is a fault-tolerance technology, minimizing service interruptions due to hardware failure or planned maintenance. In many ways, failover clustering has suffered from an image problem. Failover clustering works well technically, but its perceived configuration and maintenance complexities scare off many potential users.

## Difficult to Set Up and Use

The most common complaint I hear about failover clustering is that it's difficult to set up and use. This view stems from the pre-Windows Server 2008 days of high availability when creating a cluster was a fear-inducing procedure that required many pages of wizard input and huge amounts of configuration detail. Clustering generally required an expert, and you had to perform tasks on each node of the cluster. Once you'd actually created the cluster, maintenance was the next challenge and, once more, you probably needed a cluster specialist. And all of this is assuming you could actually get hardware that was on the cluster-supported list.

Microsoft went back to the drawing board with Server 2008 and started from scratch on many user interface elements, including management and cluster creation. The company also simplified hardware requirements to make clustering more accessible. Windows Server 2003 has a number of different quorum models to cater to different scenarios, such as File Share Witness, which was needed for clusters with no common storage. File Share Witness was initially required for Exchange Cluster Continuous Replication. Server 2008 merged all the different quorum models into a single unified model that could run in different modes but was far simpler to understand.

The cluster creation experience in Server 2008 consists of launching the cluster creation wizard and specifying the servers that will be in the cluster, a name for the new cluster, and an IP address if DHCP isn't configured on the NICs. That's it, three dialog screens in total. The cluster creation performs an analysis of the servers being added to the cluster, ascertains the availability of common storage, architect the correct mode for quorum based on storage and number of nodes, and configures all of the nodes in one step. There's no need to go to each node to set up the cluster. Also, there's a validation stage as part of the cluster creation that checks your hardware and configurations. Assuming validation passes (which is likely, as long as your nodes are running the same processor architecture, version of Windows, and so on), your cluster is supported by Microsoft, with no need to check a Microsoft Hardware Certification List (HCL) for your cluster or server hardware.

Ongoing management is just as simple. Any time you need to make a change, there are wizards to guide you through the modification. If you have a problem, running the validation again often gives good insight to the cause of the problem. This information is further improved with Server 2008 R2, and Server 2008 R2 also gives you full PowerShell management support for clusters.

## Failover Clustering Downtime

A common misunderstanding about failover clusters that causes frustration relates to downtime. There's a distinction between high availability, which failover clustering provides, and fault

tolerance, for which failover clustering can be only a part of the solution.

Failover clustering provides a framework of capabilities that services and applications can take advantage of in different ways. At the most basic level, failover clustering keeps an eye on all the nodes in the cluster. If one node becomes unavailable, clustering moves the services and dependent resources from the dead node and distributes them through the rest of the cluster, onto the remaining healthy nodes. With this basic usage of failover clustering, you'll see some downtime when the node hosting a service or application crashes. That crash has to be detected. Then the resources the node had mounted, such as LUNs, must be mounted on a new target node, and the service or application has to be restarted. All of these steps take time, so the service will be unavailable for a while. This would be common for something like a file or print service that's hosted as part of a cluster. It's also the case with services such as Exchange Server 2007 and Exchange 2003 Single Copy Cluster. The key fact is that failover clustering technology will get the service restarted and available again as quickly as possible, providing high availability, but not 100 percent availability.

When people talk about fault tolerance, they're talking about a configuration that can tolerate a failure with no service downtime to the end user. Fault-tolerant solutions typically require far more complex architectures than failover clustering, because they have to facilitate services running on multiple nodes at the same time. They also have to keep data synchronized between nodes in real time and provide failure detection and failover processes to minimize any downtime to the point that it isn't noticeable. The inbox failover clustering can't do this for services and applications using Windows-only functionality because of the differences in implementation that are required for all the different ways applications can work.

Failover clustering provides the basic infrastructure that applications and services can build on to provide fault-tolerant solutions, but that's not to say that applications can't be fault tolerant without failover clustering. Many services are fault tolerant

without failover clustering, such as Active Directory (AD) and IIS farms that use network load balancing.

A good example is Exchange 2010's database availability groups. DAGs use failover clustering behind the scenes for certain aspects of resource availability. They then add additional technology to

## Microsoft went back to the drawing board with Server 2008 and started from scratch on many user interface elements, including management and cluster creation.

replicate mailbox database data to multiple servers and provide client communication points in the form of Client Access servers that present the data to the clients from the mailbox servers. If you're seeing short periods of downtime when a node fails, this probably isn't a problem—it's by design.

### Creating a Cluster Over Multiple Locations Without Expensive Network Solutions

Cluster-enabled services typically have a number of resources allocated to them, including an IP address. Within a single location, you can have multiple nodes connected to the same network segment, or at least network segments that can be in the same IP subnet. This means the IP address for the service can be hosted on any node in the cluster, because they all have the same network connectivity capabilities. Now imagine you want to spread a cluster with nodes in multiple locations. Multiple locations typically means different network segments and IP subnets. This is a problem because you can't have a cluster resource IP address of 192.168.1.10 being hosted in a location that is subnet 192.168.10.0—the

routing just wouldn't work. The solution to this problem has been to stretch subnets across multiple locations, which typically involves very expensive network implementations, prohibiting all but the largest companies from using clustering in multi-site scenarios.

Server 2008 introduced a key change that brought multisite clustering to everyone, and it can be summed up in one word: *or*. Before Server 2008, you could allocate multiple IP addresses to a service or application as part of the resource group, but all the IP addresses had to be present—they all had to be functional on all nodes in the cluster. The Server 2008 introduction of the *or* operation means you can allocate multiple IP addresses to a service or application and specify an *or* relationship. The *or* command lets you allocate multiple IP addresses to cater for the various IP subnets the service might run on in multiple locations. The IP address that matches the location where the service is currently active is used for client connectivity, which now means you can have multi-site clustering without the expensive network solutions.

Just because you can allocate multiple IP addresses in an *or* relationship doesn't mean all your multi-site problems will be magically solved. When you have a single IP address for a service, the clients always know the address to talk to the service. If you have multiple IP addresses for a service, the solution is more complicated. You might need to use services, such as DNS, with very short Time to Live (TTL) values on the hostname records, so clients don't cache old IP addresses, or use the option to register all IP providers so all IP addresses are registered in DNS. More likely, you might use some kind of middle communication tier for the clients, such as (going back to the Exchange 2010 example) the Client Access server role.

### High Availability at the Virtualization Level vs. the Application Level

A basic piece of guidance will help you make the decision between high availability at the virtualization or application level. The trend is to virtualize everything you can, and the major virtualization solutions offer high-availability services that work in



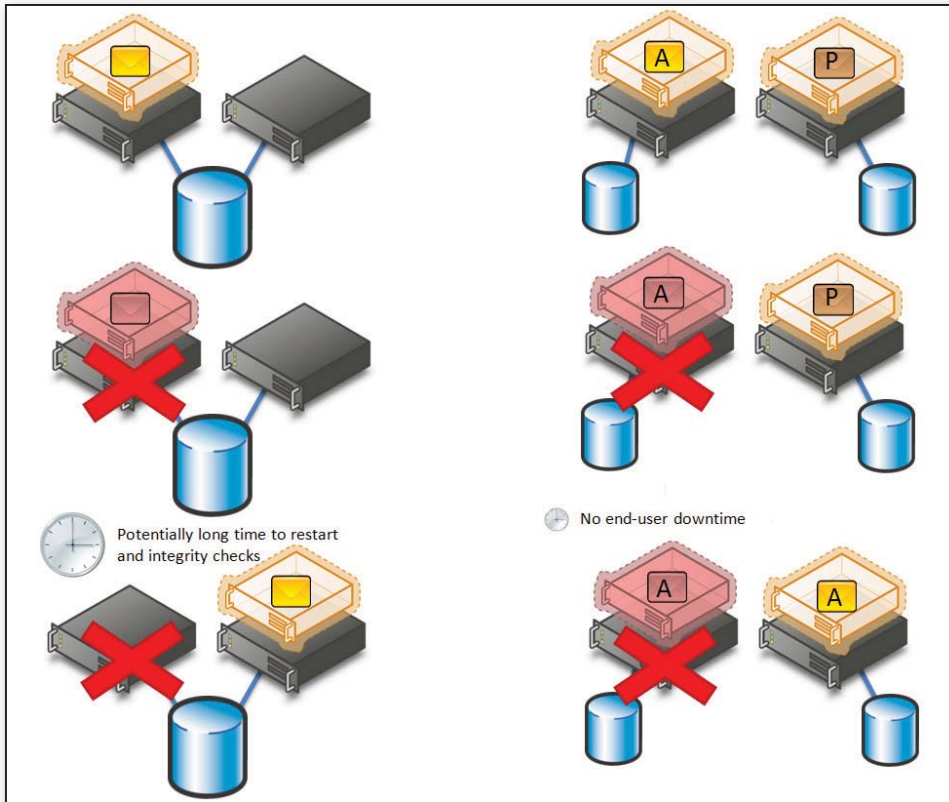


Figure 1: High availability implemented at the virtualization layer, left, and within the guest OS, right

both planned and unplanned situations. In a planned situation, for example, you might want to install a patch that requires a reboot to a Hyper-V server. You can use the Hyper-V Live Migration function to copy the memory and state of the running virtual machines (VMs) to another Hyper-V server and avoid any VM downtime.

Unplanned scenarios, in which the virtual server just crashes, don't give you time to copy the VMs' memory and states to other virtualization servers, so the VMs have to be restarted on a new virtual server in a crash-consistent state. The services offered by the VMs will be unavailable while the guest OS boots and the services start. So with virtualization you have the option of high availability at the virtualization level, but with unplanned server downtime, you'll have a period of unavailability.

The alternative is to enable high availability within guest OSs using traditional technologies, such as failover clustering, with the applications. This requires that the applications support failover clustering. If they do, application-aware high availability will generally offer far less downtime than

would be associated with restarting the OS (which you have to do with virtualization high availability).

Consider an Exchange mailbox server that's made highly available through the virtualization layer and one that's made highly available within the guest OS. When using virtualization high availability, you install one instance of the Exchange mailbox server role on a VM, with its configuration and virtual hard disks on shared storage. You make the VM highly available through the virtualization features (in the case of Hyper-V, failover clustering is actually used on the Hyper-V hosts). If the server hosting the VM crashes, another server will restart the VM in exactly the same way a physical box has to reboot after a crash. There would be a possibility of disk and database corruption due to improper shutdown, so it might need to run integrity checks, which can be very slow. This scenario is illustrated in the left side of Figure 1.

If you instead employ Exchange's high-availability features, illustrated in the right side of Figure 1, which use failover clustering in the guest OSs, you have two instances

of the Exchange mailbox server role (with Exchange 2010, you can have up to 16 in a cluster or DAG). It's critical that each instance be on separate servers—you're not adding much benefit hosting both instances on the same physical box. You should add anti-affinity rules to ensure the instances don't run on the same box. You don't need to use shared storage.

Each instance runs the Exchange software. Logs ship from the active copy of the database to the passive copy and replay there, keeping the databases synchronized. If the server that's hosting the active copy crashes, the guest OS will see that the active Exchange mailbox server is no longer responding and take ownership of the mailbox server IP and name resources. It will try to copy any missing transaction logs, check with hub

transport to make sure no messages have been lost, and start offering mailbox services from its own copy of the database. This method is much faster and cleaner than high availability at the virtualization layer.

In general, if you're running an application that supports high availability, such as Exchange or SQL Server, it's better to enable high availability at the application level within the guest OSs to achieve the optimum high availability. If you have an application that doesn't support high availability, enabling high availability at the virtualization layer is the next best thing.

InstantDoc ID 103534



## John Savill

(john@savilltech.com) is the director of Hitachi Consulting Services, the author of the popular FAQ for Windows, and a contributing editor to Windows IT Pro. He's an MCITP: Enterprise Administrator for Windows Server 2008 and an 11-time MVP. His latest book is *The Complete Guide to Windows Server 2008* (Addison-Wesley).



# 5 SharePoint Frustrations You Can Overcome

Use these workarounds to solve common annoyances

by Michael Noel

Microsoft's 2007 wave of SharePoint Products and Technologies—including Windows SharePoint Services (WSS) 3.0 and Microsoft Office SharePoint Server (MOSS) 2007—contains robust document management, collaboration, and web content management capabilities right out of the box. Over the years, however, organizations that have deployed SharePoint 2007 have vocalized certain annoyances about the product. These annoyances don't amount to insurmountable obstacles, but they can prove to be discouraging to administrators charged with maintaining and optimizing a SharePoint environment.

Every SharePoint administrator probably has a unique list of frustrations, but I've come up with a list of the most common annoyances that I've encountered. Most of these problems have workarounds that administrators can use to mitigate their effect; others require the help of a third-party solution.

## Global Navigation

By default, built-in links and navigation to SharePoint sites don't extend beyond the site collection level. In other words, each site collection acts as a navigational island, showing only links to sites within the individual site collection. Clicking the Home button in a site collection takes a user to the root of a site collection—not to the root of the web application. This idiosyncrasy can be confusing to end users, especially in environments that have many site collections.

Best scalability practice is to deploy multiple site collections—to spread them among content databases and to provide for better manageability. So, many SharePoint administrators find themselves with no obvious way to create a single seamless web experience for their users, with one Global Navigation solution for all site collections within a web application.

Microsoft provides the ability to modify Global Navigation by using a SiteMapProvider—specifically, the `Microsoft.SharePoint.Navigation.SPXmlContentMapProvider`—and by modifying the master page to reference the custom SiteMapProvider. However, this isn't a solution that users can modify within the default GUI. You can find further information about this SiteMapProvider in the Microsoft article "SPXmlContentMapProvider Class (Microsoft.SharePoint.Navigation)" at [msdn.microsoft.com/en-us/library/microsoft.sharepoint.navigation.spxmlcontentmapprovider.aspx](http://msdn.microsoft.com/en-us/library/microsoft.sharepoint.navigation.spxmlcontentmapprovider.aspx).

## Content Database Management

All SharePoint content is stored in a series of content databases residing in a Microsoft SQL Server database. These content databases store all documents, list data, web parts, and other customizations and are therefore a crucial component of a SharePoint environment. Unfortunately, however, Microsoft—by default—deploys only a single content database for a new web application, and

many organizations have let this single database grow larger than 100GB (the maximum recommended size for a content database).

To work around this problem, Microsoft recommends creating more than one content database and deploying content across multiple site collections. The downside is that there's no way in the GUI to determine which database a new site collection will go into. Trying to organize content by

to leave SharePoint and use a different tool such as the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in to determine the membership of the group.

There's no easy, native way to overcome this limitation from within SharePoint, but there are third-party administration solutions for SharePoint and custom-built utilities that perform LDAP lookups against AD to help

which makes the indexing component non-redundant and requires setting up scenarios involving index servers in different farms, indexing content from other locations. Other farm architectural limitations restrain the scalability of SharePoint in ASP models—most notably the requirement that every web role server contain every web application in that farm, which significantly increases overhead and reduces the number of web applications that can be deployed.

The good news is that SharePoint 2010 does away with the concept of the SSP. The new version replaces SSPs with a Services model, in which every shared service has a corresponding SQL Server database that farm members utilize. In addition, the restriction of having all web applications on every web role server is gone.

The bad news is that these annoyances are difficult to address in SharePoint 2007. However, administrators have had some success with third-party solutions for making the index component redundant and scaling SharePoint by creating multiple farms. Management of these types of environments can be cumbersome once you reach a certain scale, however, which explains why SharePoint 2010 kills SSP.

## Overcome Limitations

Every technology has its annoyances, making its users wonder what the developers were thinking! This article is by no means an exhaustive list of all the SharePoint idiosyncrasies that can lead administrators to yank out their hair, but it should provide an understanding of some common problems. With a good understanding of SharePoint's limitations—and the right workarounds—you can overcome the inherent annoyances. And we can all look forward to the inevitable improvements in SharePoint 2010.



InstantDoc ID 103567

**The good news is that SharePoint 2010 does away with the concept of the SSP. The bad news is that SSP-related annoyances are difficult to address in SharePoint 2007. But solutions are out there.**

database—for example, giving a specific department its own content database—can get frustrating.

There are two possible solutions to this problem. The first solution is the easiest, but it applies only when you're creating a site collection in a new content database. For this scenario, simply create the site collection using the Stsadm command-line utility and use the -createsiteinnewdb switch. For existing content databases, simply increase the maximum number of sites that can be created in that database under the Content Databases link in the SharePoint Central Admin tool. Set the number to be much higher than any other database, and SharePoint will automatically home the site collection there.

## AD Group Membership Lookups

Although SharePoint can tie into and use Active Directory (AD) security credentials for authorization, there are limitations to this concept when you use AD groups for granting security rights. If an administrator wants to grant all the members of an AD group rights to a site collection, for example, he or she can add them from within SharePoint, but there's no way within the administrative interface to determine who is a member of a specific group. Instead, the administrator needs

overcome this annoyance. One solution, an RSSBus web part ([www.rssbus.com/products/sharepoint/templates/template.aspx?webpart=ldap.ListGroups](http://www.rssbus.com/products/sharepoint/templates/template.aspx?webpart=ldap.ListGroups)), allows for this type of functionality.

## Multiple Authentication Prompts

Depending on the method by which users access SharePoint, and the security settings of the browser, users might end up having to authenticate multiple times throughout their session. This problem is particularly true when a Microsoft Office client such as Word or Excel is in use.

Fortunately, this annoyance is fairly well documented and can typically be resolved by changing browser security to automatically use the user's credentials or reuse the credentials initially used. For most organizations, this means adding the SharePoint server URL to the Local Intranet security zone in Internet Explorer (IE), which should remove most repeat authentication prompts.

## Shared Services Provider and Farm Scalability

The concept of the Shared Services Provider (SSP) in SharePoint 2007 creates a host of scalability annoyances that SharePoint administrators have been dealing with for years. For example, there can be only one index server per SSP,



### Michael Noel

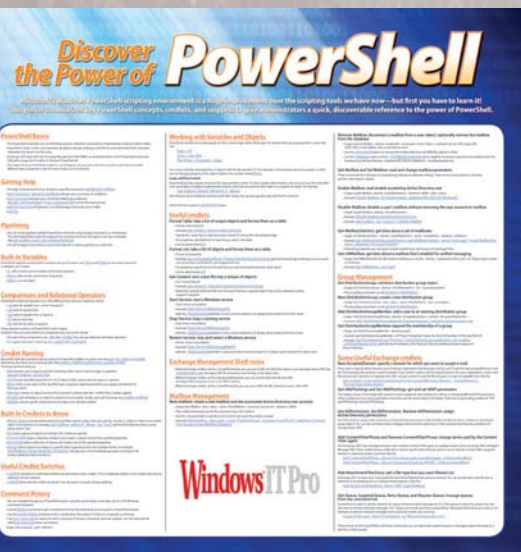
([michael@cco.com](mailto:michael@cco.com)) is a partner at Convergent Computing, a Microsoft SharePoint MVP, and the author of books on SharePoint, ISA Server, and Exchange Server. His latest book is *Windows Server 2008 Unleashed* (Sams).



# Prime Your Mind

with Resources from Left-Brain.com

Left-Brain.com is the online superstore stocked with educational, training, and career-development materials focused on meeting the needs of IT professionals like you.



## Featured Product:

### Windows PowerShell Poster Discover the Power of PowerShell

Microsoft's Windows PowerShell scripting environment is a huge improvement over other scripting tools, and we can help you learn it! Our new PowerShell poster summarizes key PowerShell concepts, cmdlets, and snippets for group management, Exchange, and other admin tasks.

Topics covered are PowerShell basics, pipelining, built-in variables, mailbox management, command history, and much more!

**Only \$14.95\*!**

Order your poster and discover other great PowerShell resources now at Left-Brain.com

\*Plus shipping and applicable tax.



[www.left-brain.com](http://www.left-brain.com)

Windows IT Pro

# XP to Windows 7 Migration with Microsoft Deployment Toolkit 2010

With the right tool, it's easy to deploy a new OS to several machines

by Rhonda Layfield

**B**y now, you've probably heard that there isn't a direct upgrade path from Windows XP to Windows 7. When installing Windows 7 on a machine that runs XP, you can choose to wipe the hard disk clean and install a fresh copy of Windows 7 or you can perform a migration. Migrating allows you to install Windows 7 while maintaining your users' settings and data. Applications that are installed on the XP machine won't be migrated—you'll have to redeploy them using Group Policy or Microsoft System Center Configuration Manager.

Although migrating one or two machines is no big deal, migrating 20 or 20,000 XP machines can be a real pain. This article is designed to help ease that pain by showing you how to set up a repeatable migration solution so every migration you perform is identical to the last, other than the user settings and data stored locally on the XP machines. Microsoft's free deployment tool, Microsoft Deployment Toolkit 2010 (MDT 2010), provides friendly wizards that walk you through scenario-based questions. Then, under the hood, based on the answers you gave the MDT wizards, MDT does all the hard work for you.

MDT isn't a new tool—it used to be called Solution Accelerator Business Desktop Deployment Tool (BDD). Since then, it's had a lot of the kinks worked out. If you found it difficult to use earlier versions of

## PROBLEM:

You need to migrate several Windows XP machines to Windows 7.

## SOLUTION:

Use Microsoft Deployment Toolkit 2010.

## WHAT YOU NEED:

Microsoft Deployment Toolkit 2010, Windows Automated Installation Kit for Windows 7

## SOLUTION STEPS:

1. Install MDT
2. Create a deployment share
3. Import your OS
4. Create a task sequence
5. Update the deployment share
6. Deploy your first image

## DIFFICULTY:



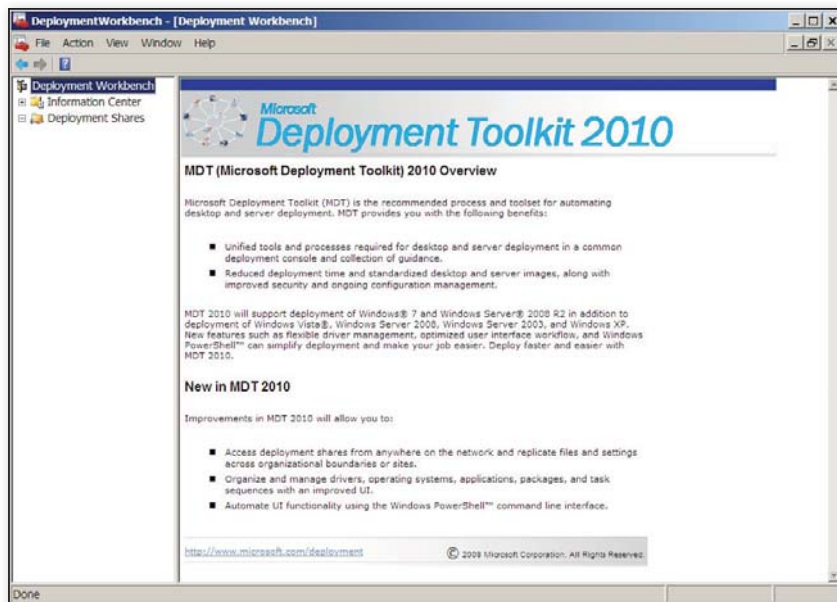


Figure 1: The Deployment Workbench snap-in

MDT or BDD, I think it's safe to say you'll be pleased with this version. It's definitely worth another look.

In this article, I'll give you step-by-step instructions to install MDT, create a deployment share, import an OS, create a task sequence for migrating XP SP2 and SP3 to Windows 7, and finally walk you through the migration process. This process is also known as a refresh scenario because you're refreshing the same piece of hardware with a new OS.

## Step 1: Install MDT

Installing MDT 2010 doesn't require a big beefy machine. MDT requires a 1.4GHz processor, 2GB of RAM, a Gigabit NIC if you'll be deploying multiple machines concurrently, enough hard disk space to store your images (I suggest at least 20GB to get started), and RAID if you want to provide fault tolerance for your images.

MDT requires the Windows Automated Installation Kit for Windows 7 (WAIK 2.0). It doesn't matter whether you install MDT or WAIK first, but MDT won't be able to deploy anything until WAIK is installed. WAIK requires Microsoft XML Core Services (MSXML) 6.0 and .NET Framework 2.0 or later if installing MDT on older OSs; newer OSs such as Windows Server 2008 and Server 2008 R2 have MSXML 6.0 and .NET Framework built-in. Don't worry, both MSXML 6.0 and .NET Framework 2.0 are included in the WAIK download.

Before I get started, there are some terms you should be familiar with. Installing MDT on Windows 7 or Windows Vista SP1 creates a *technician machine*. Installing MDT on a server OS (Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003 SP2) creates a *deployment server*. I recommend installing MDT on a server OS (latest and greatest is the best) so you get all the bells and whistles that the server OS brings to the table, such as easy integration with Windows Deployment Services (WDS). The OSs that MDT 2010 supports for deployment are Windows 7, Windows Server 2008 (including all service packs and R2), Windows Vista (SP1 or later), Windows Server 2003 R2, and Windows XP SP2 and later. The *target machine* is the machine to which you're deploying the new OS. In this article, your XP workstations are the target machines.

After you've installed MDT, you'll use the Deployment Workbench (DW) snap-in, shown in Figure 1, to do all your work. You'll find the DW under Start, All Programs, Microsoft Deployment Toolkit, Deployment Workbench.

## Step 2: Create a Deployment Share

A deployment share is the shared folder your target machines connect to during the deployment process, so you'll need to be sure your machines have network connectivity and permissions to the deployment share. You can have as many deployment

shares as you choose. Create a deployment share within the DW by right-clicking the Deployment Shares node and choosing New Deployment Share. The New Deployment Share Wizard opens. Follow these steps to create your new deployment share:

1. On the Path page, click the Browse button and navigate to the folder in which you'd like the new deployment share to be created, or type the path. No need to create the folder first—MDT is smart enough to create it for you. I recommend creating your deployment share on a volume other than the system volume. Another hard disk would be even better. My deployment share will be created in the F:\DeploymentShare folder. Click Next.

2. On the Share page, type the name you'd like for the shared folder name. Accepting the default will name the deployment share's shared folder DeploymentShare\$. (The \$ at the end of the share name makes this a hidden share, so the folder name won't show up on browse lists.) Click Next.

3. On the Descriptive Name page, you can give your shared folder a description. The description can be seen from a browse list if you removed the \$ from the shared folder name in step two or when you list the shares on a deployment server. An easy way to list the shares on the deployment server is to open a command prompt and type *net share*—your description will be in the Remark field. After you input your deployment share description, click Next.

4. Next is the Allow Image Capture page, which by default is configured to ask if an image should be captured of the target machine before installing Windows 7. Accepting the default setting will cause the deployment wizard to ask you whether an image should be created of the target machine and, if so, where the image (a .wim file) should be stored. This is helpful if you need to roll back the target machine to its original image. Accept the default setting and click Next.

5. By default, the Allow Admin Password page is set not to ask users to set the local administrator password during the deployment. This setting, if left at the default, will assign the target machine's local administrator account a blank password. That's not the whole story, however—there are other ways to provide



the local administrator password. In my example, I'll provide it in a task sequence I'll create later in this article. Accept the default setting and click Next.

6. The Allow Product Key page allows you to choose whether you want to be prompted for a product key during the deployment process. Enterprise clients won't need to worry about product keys because theirs are baked into the OS files. For non-enterprise clients, I recommend accepting the defaults on this page and typing the product key into your task sequence (like with the local administrator password, as I mentioned in step five). Clicking Next takes you to the Summary page.

7. The Summary page displays the choices you've made in the New Deployment Share Wizard. Clicking Next on the Summary page begins creating the deployment share. The steps run to create a deployment share are displayed in the Progress page that appears rather quickly then disappears, leaving you at the Confirmation page.

8. There are two buttons on the Confirmation page that are new to MDT 2010, Save Output and View Script. Clicking the Save Output button lets you store the output, which is exactly what you see on the confirmation page. The View Script button shows the Windows PowerShell commands that were run to create the deployment share. You can copy and paste commands to create your own PowerShell scripts.

When the New Deployment Share Wizard has completed successfully, your new deployment share will appear in the

DW under the Deployment Shares node, as shown in Figure 2. When you expand your new deployment share, you'll see six nodes: Applications, Operating Systems, Out-of-Box Drivers, Packages, Task Sequences, and Advanced Configuration. I'll show you two of these nodes: Operating Systems and Task Sequences, with the Operating Systems node first.

### Step 3: Import Your OS

Before you can deploy an OS, you'll need to import one into the DW. No matter which OS you import, the steps are all the same. To import an OS, right-click the Operating Systems node and choose Import Operating System to open the Import Operating System Wizard. Follow these steps in the wizard:

1. On the OS Type page, select *Full set of source files*. You can add custom image (.wim) files that you've created and WDS OS images later. Click Next.
2. On the Sources page, click the Browse button to navigate to your full set of source files. You can use either the root of a Windows 7 DVD or a folder where you've copied the entire Windows 7 DVD.
3. The Destination page prompts you for the name of the folder in which you'd like to store this OS. The folder will be created in your deployment share's OS folder. In my case, it's F:\DeploymentShare\Operating Systems. Don't look for this folder in the DW; you won't find it there. You can find it by using Windows Explorer and navigating to the deployment share you created in the previous section. Click Next.
4. The Summary page displays the details of the Import Operating System

Wizard, just as the New Deployment Share Wizard did. After reviewing your choices and making any necessary changes, click Next.

5. The Progress page appears. When the OS is imported, the Confirmation page appears. Importing image files can take a while, depending on the size of the image and speed of your server. Click Finish on the Confirmation page and your newly imported OS will be displayed in the DW under the Operating Systems node.

At this point, I have to mention one of my favorite new features in MDT 2010. I can now organize my OSs by creating folders to store them in. For example, you could create a folder under the Operating Systems node by right-clicking Operating Systems and choosing New Folder. Give the folder a name (such as Win 7 or XP), click Next twice, then Finish. Then you can move the OSs you've imported from one folder to another by cutting and pasting. You can create similar folder structures for your applications, drivers, and packages to keep things more organized, as shown in Figure 3. You can import applications, drivers, and packages in much the same way that you imported the OS, but with different options.

### Step 4: Create a Task Sequence

The task sequence is where things start to get interesting. A task sequence contains a list of tasks to be performed during the migration and the order in which they will run. To create a task sequence, right-click the Task Sequence node and choose New Task Sequence to launch the New Task Sequence Wizard. Then, follow these steps:

1. On the General Settings page, fill in the Task sequence ID, Task sequence name, and Comments. For example, my Task sequence ID is W7x64 and my Task sequence name is Windows 7 64-bit. The comments field is a great way to document information about the task sequence, such as when it was created, why it was created, and what will be deployed using this task sequence. Clicking Next takes you to the Select Template page.
2. The Select Template page lists the built-in templates. Choose Standard Client Task Sequence from the drop-down menu and click Next.

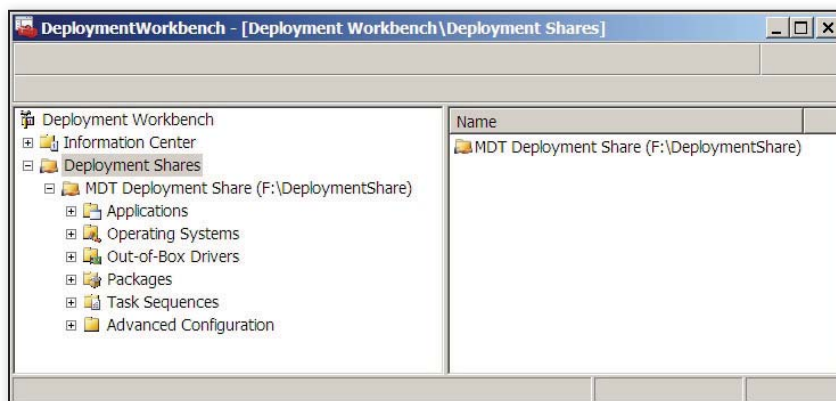


Figure 2: The new deployment share in the DW

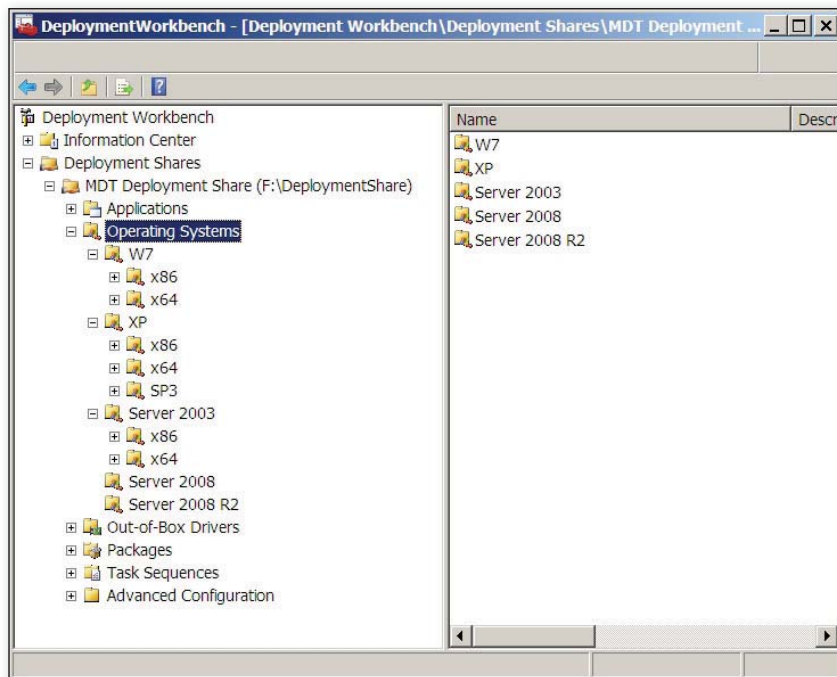


Figure 3: Organizing your Deployment Workbench

3. Select the OS (Windows 7) you'd like this task sequence to deploy on the Select OS page, then click Next.

4. On the Specify Product Key page, input a product key if needed (if you choose not to specify a product key at this time, you'll be prompted to enter one during deployment), then click Next.

5. The OS Settings page provides fields for Full name, Organization, and Internet Explorer home page, all of which are required fields. Fill these fields in and click Next.

6. Provide a password to be used for the target machine's local administrator account on the Admin Password page. Remember that when I created the deployment share, I left the Allow Admin Password page at the default, not to prompt for a local administrator password (step 6 in the Create a Deployment Share section). If you choose not to specify an administrator password at this time, when the migration is complete, the Windows 7 local administrator password will be blank. Input a password and click Next.

7. The Summary page gives you the opportunity to review your choices. When everything looks good, click Next. The Progress page appears and displays the steps being run to create the task sequence. When finished creating the task sequence,

the Progress page disappears and the Confirmation page appears.

8. On the Confirmation page, click Finish.

### Step 5: Update the Deployment Share

Updating your deployment share is when the gears of MDT start to turn. When you update your deployment share, the tools needed by MDT are copied into your deployment share. Quite a few other things occur too, but they are outside the scope of this article. Follow these steps to update your deployment share:

1. In the DW, expand the Deployment Shares node. Right-click your deployment share name and choose Update Deployment Share from the menu.

2. The Update Deployment Share Wizard launches and displays the Options page, shown in Figure 4. There are two options to choose from: *Optimize the boot image updating process* and *Completely regenerate the boot images*. The first time you update the deployment share, it doesn't matter which option you select because either option will do the same thing. Accept the default option, then click Next.

3. In the Summary page, review your selections, make any necessary

changes, and click Next. The Progress page appears and shows you the steps performed to update the deployment share. When the deployment share is updated successfully, the Confirmation page appears. Click Finish on the Confirmation page to complete the Update Deployment Share Wizard.

Now you're ready to migrate your very first XP machine to Windows 7. Make sure that your target machine has networking functionality and can connect to the MDT deployment server's deployment share.

### Step 6: Deploy Your First Image

To migrate your XP target machine to Windows 7, you'll need to begin by booting the machine into XP and logging into your domain. Then you'll need to connect to the deployment server and run LiteTouch.vbs to kick off the migration. Follow these steps:

1. On the XP target machine, click the Start button, then Run. Type the Universal Naming Convention (UNC) path to a script named LiteTouch.vbs stored in your deployment share's scripts folder. My deployment server's name is 2010Server and my deployment share is DeploymentShare\$, so my UNC path is \\2010Server\DeploymentShare\$\Scripts\LiteTouch.vbs

2. When LiteTouch.vbs launches, the Windows Deployment Wizard begins. There are two options on the first page, but only one is selectable: *Refresh this computer*. The *Upgrade this computer* option isn't selectable because there's no upgrade path from XP to Windows 7, only migration. Accept the default selection and click Next.

3. The current name of the XP machine appears on the *Configure the computer name* page. You can accept the existing name or provide a new name. Click Next.

4. The *Join the computer to a domain or workgroup* page allows you to input credentials for joining the new Windows 7 machine to your domain or a workgroup. You can even specify the Active Directory organizational unit (OU) where you'd like to create the new computer object, but you'll have to use the distinguished name. For example, if my domain is named deploy.com and I want the new computer object to be created in the Workstations OU (which I've previously created), my

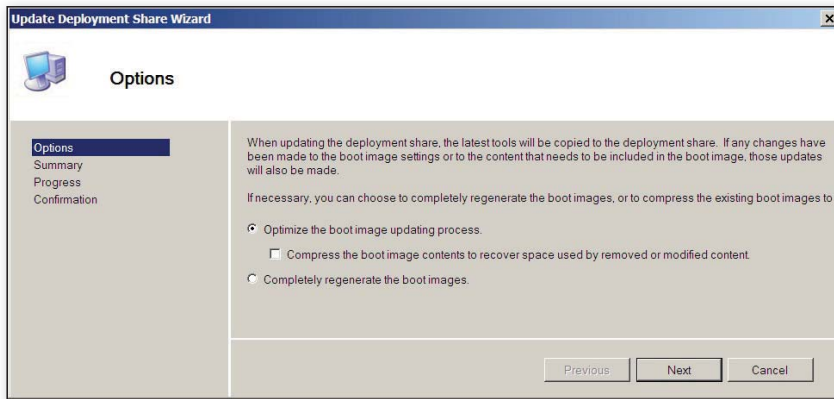


Figure 4: The Update Deployment Share Wizard options

distinguished name would look like this:  
OU=Workstations,DC=Deploy, DC=com.

5. After making your selection to join a domain or workgroup, click Next.

6. There are three selections on the *Specify where to save your data and settings* page—*Automatically determine the location*, *Specify a location*, and *Do not save data and settings*. The *Automatically determine the location* setting has a sub-setting, *Allow data and settings to be stored locally when possible*. If both are selected, the User State Migration Tool (USMT) Scanstate utility will run utilizing the new USMT v4 hard link option. The hard link option identifies user's settings and data stored locally and stores information about them (such as where they reside on the local hard disk) in the C:\MININT\StateStore\USMT folder. The actual files and settings are left completely intact while the XP OS files that surround the settings and data are replaced with Windows 7. In a refresh scenario, this is possible because the hard disk never gets formatted. (There's no way to use hard links and format the system drive—the hard link data would be stored first, then the process of formatting the hard disk would wipe out the data.)

7. Choosing *Specify a location* requires that you provide a UNC path for where you'd like to store the user's settings and data. Storing the user's settings and data on a network location creates network traffic and the need for storage space. Storing the user's settings and data locally using USMT hard links cuts down on both network traffic and the amount of storage space needed. I'll store mine on the deployment server in the shared USMT folder (you'll have to create and share the USMT folder first). I also want

each computer to create a folder within the USMT folder based on its computer name (I'll use the %ComputerName% variable). My target machine is named XPTIStaff, so my UNC path is \\2010Server\USMT\%ComputerName%. The third option, *Do not save data and settings*, will do just that—save nothing.

8. The *Specify where to save a complete computer backup* page gives you the opportunity to create a .wim image of the

## MDT is capable of much more than just migrating XP SP2 and later machines to Windows 7 while maintaining your users' settings and data.

XP machine before replacing the OS with Windows 7. You have the same options as the last page: *Automatically determine the location* (if there's room, the .wim image will be stored locally and not be overwritten when the new OS is deployed); *Do not back up the existing computer*; and *Specify a location* by using a UNC path for where you'd like to store the .wim image file. For example, I have a folder shared as Backups on my deployment server, so I typed the UNC path \\2010Server\Backups.

9. On the *Language and other Preferences* page, fill in settings such as language and time and currency formats, then click Next.


10. Select your Time Zone and click Next.

11. Choose any applications you'd like to install on the *Select one or more applications to install* page. You need to add applications to the DW before they'll appear on this list. Click Next.

12. The *Specify the BitLocker configuration* page lets you choose whether to enable BitLocker on the target machine. If you choose to enable BitLocker, you can also specify where to store the BitLocker encryption key. Accept the default setting, *Do not enable BitLocker for this computer*, and click Next.

13. The *Ready to Begin* page is the last page in the deployment wizard. Clicking Details shows your selections. After reviewing your settings (make changes by clicking the blue circle with the back arrow in the bottom left corner), click Begin and let it rip. The deployment begins and displays the Installation Progress bar that shows each stage of the installation.

Under the hood, USMT runs Scanstate and stores the user's settings and data in the path you provided. Then the XP target machine reboots into a custom MDT Windows Pre Installation Environment (WinPE). This custom MDT WinPE contains the scripts needed to deploy Windows 7. After Windows 7 is installed, USMT runs again and this time performs a loadstate command that will migrate the users' data and settings from the \\2010Server\USMT\ITStaff folder. If the migration completed successfully, you'll see a screen telling you so.

MDT is capable of much more than just migrating XP SP2 and later machines to Windows 7 while maintaining your users' settings and data. But for now, I hope these steps will help ease the migration pain. 

InstantDoc ID 103607



### Rhonda Layfield

(rhonda@minasi.com) is a consultant, trainer, Setup and Deployment MVP, and desktop deployment product specialist.



# Preparing to Deploy Exchange 2010

Get your OS, hardware, and other infrastructure details right, before rushing to install the new software

by Tony Redmond

**N**ew software brings new challenges, and Microsoft Exchange Server 2010 is no different. The urge to take the shrink-wrap off the new software is intense, but foolish administrators rush to deploy where hard-bitten and scarred practitioners pause for thought. Before deployment can begin, you need to understand the prerequisites that exist and the obvious pitfalls to avoid. This article describes what you need to do to prepare to deploy Exchange 2010 into new or existing organizations.

## Get the OS Right

A solid implementation of the OS provides the foundation of any successful deployment. Exchange 2010 supports both Windows Server 2008 SP2 and Server 2008 R2. The most sensible option is to deploy on Server 2008 R2 because Microsoft doesn't support an OS upgrade after you install Exchange 2010 on a server. Thus, you can deploy Exchange 2010 and Server 2008 SP2 and plan for a complete refresh subsequently, or you can deploy Exchange 2010 and Server 2008 R2 and anticipate stability at least until the next major release of Exchange or Windows Server appears.

You'll have to deploy other software to create the right environment for Exchange 2010, including Windows Remote Management, the latest version of the .NET Framework, Windows PowerShell 2.0, various Windows components such as the Active Directory (AD) management tools, and various server roles. See the Microsoft article "Exchange 2010 Prerequisites" ([technet.microsoft.com/en-us/library/bb691354\(EXCHG.140\).aspx](http://technet.microsoft.com/en-us/library/bb691354(EXCHG.140).aspx)) for more information.

If you scan the Internet, you'll find scripts that others have written to prepare servers for Exchange 2010, mostly by installing the long list of server features that Exchange depends on. I've used the script posted at [www.ucblogs.net/files/folders/powershell/entry125.aspx](http://www.ucblogs.net/files/folders/powershell/entry125.aspx) to prepare a server, and it worked well. Be sure to test any script you download before you use it in production, and always verify that you understand what the code does because you don't want to take any chances by downloading and running unverified code.

Be sure to check for required OS upgrades and hotfixes before you install servers. Exchange touches many parts of the OS and has a track record of exposing weaknesses. Microsoft IT discovered a problem with NTFS deadlocks on heavily loaded Mailbox servers soon after they deployed Exchange 2010 internally. This problem is specific to Server 2008 SP2 and required administrators to kill store.exe to free the condition, so it was pretty serious. Microsoft released a hotfix, which you can download from Microsoft Support at [support.microsoft.com/kb/974646](http://support.microsoft.com/kb/974646), but it's a good example of the kind of problem that comes to light when new combinations of OS and applications go into production.

## Get Your Infrastructure Ready

Exchange 2010 requires AD to operate in Windows Server 2003 functional mode, so you can upgrade the forest to this level now if you haven't already done so. Exchange 2010 extends the AD schema, too. In fact, the same schema extensions are applied if you deploy Exchange 2007 SP2. If you plan to run Exchange 2010 in an existing Exchange organization, you have to make sure that legacy servers run at least Exchange 2003 SP2 or Exchange 2007 SP2 before you can deploy the first Exchange 2010 server; no Exchange 2000 servers can be present in the organization.

Microsoft has invested a lot of energy in the development of the Exchange Server Best Practices Analyzer (ExBPA) and has incorporated it into the Exchange 2010 installation procedure to run preinstallation checks to validate that you're ready to deploy Exchange 2010. If you're already running an older version of Exchange, you can take a proactive step and run ExBPA at any time to see whether your organization is functioning properly. This step won't tell you if your organization is ready to support Exchange 2010, but it will pinpoint any obvious problems that you should address before you get serious about moving to Exchange 2010.

## What to Do About Hardware

Server hardware is next on the list. Any server shipped since about 2006 should be capable of running Exchange 2010, so there's no immediate need to invest in new hardware unless you're making a move from Exchange 2003, which might still be deployed on 32-bit hardware rather than the 64-bit systems required by Exchange 2010. However, remember that you can't upgrade a server in place; you have to make a fresh start with Server 2008 R2 and Exchange 2010.

There's a natural temptation to deploy new software on new hardware. If your servers are older and becoming harder and more expensive to support—say, three years old or older—they struggle with the existing load, or they're simply not available enough because of current demand, you probably need to invest in new servers. A desire to deploy virtual servers is another reason to consider new hardware because vendors are increasingly focusing the latest multi-core servers on being great virtualization platforms.

Finally, if your current Exchange organization runs a configuration that isn't supported by Exchange 2010, you might need to upgrade your hardware. These unsupported configurations include single copy or "classic" mailbox clusters and the variants on cluster replication available in Exchange 2007. These high-availability options have all been replaced by the database availability group (DAG) in Exchange 2010. It's possible to deploy a DAG for even small installations, but we're still learning how to leverage DAGs to run on a small number of servers so you should take time to figure out your high-availability needs and then how to use the Exchange 2010 technology to satisfy those requirements.

Of course, you might be able to reuse existing servers for Exchange 2010. The usual approach would be to follow these steps:

1. Install Server 2008 R2 and Exchange 2010 on available hardware. Deploy Client Access servers first, then Hub Transport and Edge Transport servers, and finally Mailbox servers into the existing organization.
2. When the Exchange 2010 Client Access and Hub Transport servers are fully operational, remove the legacy servers.
3. When Exchange 2010 Mailbox servers are available, move your mailboxes from legacy servers to Exchange 2010, then remove the old servers.
4. As old servers are decommissioned, you can recycle the hardware to become new Exchange 2010 servers on Server 2008 R2.

Note that Microsoft doesn't provide 32-bit versions of Exchange 2010. Workstations have to run 64-bit versions of Windows 7 or Windows Vista before you can install the management components, Exchange Management Console (EMC) and Exchange Management Shell (EMS). Exchange 2010 includes a new web-based management utility called the Exchange Control Panel (ECP) that includes tasks such as recipient management (basically, working with properties of mailboxes, groups, and contacts). You don't have to install anything except a recent browser—Microsoft Internet Explorer (IE) 7.0 or later, Firefox 3.0 or later, or even Google Chrome—to be able to use ECP, but most administrators will find that the current iteration of ECP is somewhat limited and best suited to Help desk or support personnel and will need to use EMC or EMS to fully maintain

the organization. You should use 64-bit hardware for test boxes as well, although it's possible to deploy small test environments on 32-bit workstations by using virtualization software that supports 64-bit environments. And of course, you can always use RDP to connect to a server and run EMC there to perform management operations.

## Server Workload

Exchange 2010 Client Access servers do more work than their Exchange 2007 equivalents because they handle all client connections. MAPI clients are handled by a new RPC client access layer. This reorganization lets Exchange break the link between server and database, a development which is exploited by the DAG to achieve resilience against server and storage failure. In other words, all previous versions of Exchange have a fixed connection between the database that hosts a mailbox and the server where it's located. Servers in a DAG can move connections between database copies as conditions in the DAG change. The RPC client access layer directs incoming client connections to the current live database for the associated mailbox instead of always going to a fixed server. The results of full performance tests in production environments aren't yet available, but a rule of thumb suggests that you can expect a double workload for Client Access servers. Hub Transport servers boast some useful new features but generally do much the same work as in Exchange 2007 and shouldn't cause problems.

Mailbox servers benefit from the changes Microsoft made to the database schema to reduce I/O demand. However, you have to compare apples to apples to get an accurate view of server performance. You'll see the improvement if you run Exchange 2010 in exactly the same configuration as Exchange 2007. Your results will be different if you decide to exploit some of the new features such as supporting much larger mailboxes (5GB is a typical figure) or archive mailboxes. New features always consume extra resources, so be sure you understand the full context before you settle on a server configuration.

## What to Do with Storage

The reduction in I/O demand has received a lot of attention because it lets Exchange support low-cost storage. In the past, the

relatively high I/O demand exerted by Exchange servers made system designers use SAN-based storage for high-end systems. SAN-based storage has been the cornerstone of many successful corporate storage architectures, but it's expensive and complex. Exchange 2007 offers lower I/O demand than previous Exchange versions, but really only for small mailboxes (200MB or less).

Apart from some tinkering with page size in Exchange 2007, Microsoft never really bit the bullet to redesign the internal workings of the Information Store until now, but the early signs are that the new schema contributes to a much lower I/O demand—on the order of 0.25 I/O operations per second per active mailbox. This improvement, taken together with the additional resilience available through the deployment of multiple database copies in a DAG, makes it feasible to deploy disk configurations such as Just a Bunch of Disks (JBOD) arrays that would never have been considered for Exchange in the past.

### Backup and Other Third-Party Applications

Exchange 2010 doesn't support streamed backups. Instead, you have to deploy a Microsoft Volume Shadow Copy Service (VSS)-based backup solution. Now is a good time to review how you perform backups and to make any changes that are required to prepare for Exchange 2010. Check with the vendor of your current backup software about when they'll have an upgraded version. The same advice applies to any other third-party solution in your organization, including RIM's BlackBerry Enterprise Server, which definitely requires a new version to support Exchange 2010. Microsoft has made many changes to the Store and APIs in Exchange 2010, and most third-party applications need to be upgraded before they'll run properly. Some APIs, such as WebDAV, aren't supported by Exchange 2010, so applications that depend on these APIs are simply not supported.

On a positive note, it's possible some software you run now is no longer required because of the new Exchange 2010 features or improvements that Microsoft has made to the way the product works. For example, some companies deploy software that regularly rebuilds databases to free up disk space. This procedure hasn't actually been

required since Exchange 2003 because Exchange itself does a good job of online defragmentation to reuse white space in databases, so these products are good candidates to be decommissioned. Archiving software might be another candidate because Exchange 2010 lets you assign archive mailboxes to users and includes a range of other features to enable better indexing and discovery of information kept online to meet legal and regulatory requirements. All of this proves that you should take an inventory of third-party applications and ask whether you need them after Exchange 2010 is deployed. If you do, get a new version from the vendor. If you don't, be happy that you've saved some money.

### Get to Know Exchange 2010

No deployment is possible if you don't understand the software. Exchange 2010 has many changes that affect systems administration. The two biggest changes are the introduction of Role Based Access Control (RBAC) and PowerShell 2.0, which includes remote PowerShell. RBAC replaces the permissions model used in previous versions of Exchange and is designed to give administrators the correct level of access to Exchange objects to get their job done. Organization administrators have access to every object from servers to connectors to mailboxes; Help desk personnel might just be able to update recipient objects to change their phone number; and users can update only their personal information. RBAC has a much larger influence over large deployments where multiple administrators work; it's much less important for deployments managed by a few "all-powerful" administrators who likely have access to everything.

Using remote PowerShell means that rather than running PowerShell locally on a server, all access to the code that implements Exchange functionality (what the development team calls "business logic")—provided in the form of an expanded set of cmdlets—flows through Windows Remote Management, Microsoft IIS, and RBAC. Access is always remote, even when running on an Exchange server. The intention is to ensure that all connections to Exchange flow through a gate where access can be validated and tailored for the requesting user. For example, when you start EMS, RBAC determines what access

level you have and provides a tailored set of cmdlets that lets you do your work. The same happens when you start EMC: The UI includes only options that you're allowed to access.

RBAC and remote PowerShell are just two of the many changes that occur across the product, but they underscore the need for administrators to upgrade their knowledge to fully understand Exchange 2010 before they even think about installing a server.

### The Online Option

Of course, you don't have to deploy Exchange 2010 yourself. You can let Microsoft do the job for you and connect to Exchange 2010 through Microsoft Business Productivity Online Standard Suite (BPOS). Microsoft has invested a lot of engineering effort to make Exchange 2010 operate as smoothly in a hosted environment as it does for on-premises deployments, and using BPOS is a viable alternative for many companies that use Exchange only as an email server and don't have special needs for data retention, privacy, extended security, or legal and legislative functionality that's still best delivered through an on-premises deployment. At press time, Microsoft hadn't yet deployed Exchange 2010 as the basis of its BPOS service but will do so in the near future.

### Maximize the Joy

Like any major upgrade of a server application, Exchange 2010 delivers a mixture of joy, with its new features and enhancements, and pain, in the cost to prepare for and then execute the deployment. The trick is to maximize the joy while minimizing the pain, and good preparation is key to achieving this goal. Don't expect to deploy Exchange 2010 successfully without putting in the effort to understand the full context of your existing installation, including third-party applications. Take your time, prepare well, and then execute. It's much better than plunging in only to fail.



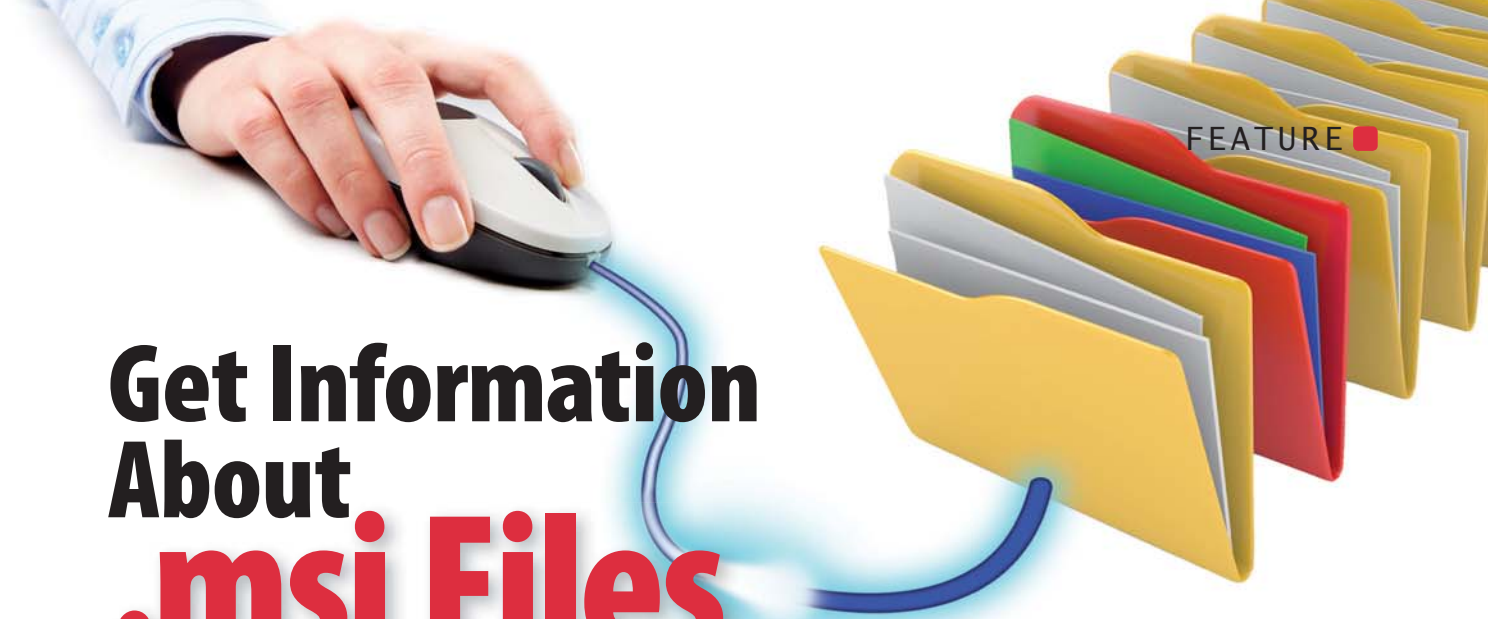
InstantDoc ID 103517



### Tony Redmond

(12knocksinna@gmail.com) is a contributing editor for *Windows IT Pro*, and author of *Microsoft Exchange Server 2007 with SP1* (Digital Press).





# Get Information About .msi Files with Just a Few Clicks

**S**uppose that a couple of years ago, you downloaded a Windows Installer package named `mwta.msi`, but you can't remember what it's for and its obscure filename doesn't provide any clues. How can you find out the name, manufacturer, and version of the software it will install without actually installing it?

Unfortunately, right-clicking an `.msi` file and choosing Properties doesn't provide much information. If you have Orca installed, you can right-click the `.msi` file, choose *Edit with Orca*, navigate to the Properties table, and look at the `.msi` file's properties. However, this is time consuming. Plus, Orca updates the last modified date of an `.msi` file after you close it, even if you don't make any changes—a behavior I find less than optimal. (If you're unfamiliar with `.msi` files and Orca, see the web-exclusive sidebar "Windows Installer at a Glance" ([www.windowssitpro.com](http://www.windowssitpro.com), InstantDoc ID 103530).

I found myself wanting a simpler solution, so I created MSIInfo, which works on Windows 2000 Server and later. This utility displays five properties for `.msi` files:

- Manufacturer, which specifies the manufacturer of the software to be installed.
- ProductName, which specifies the name of the software to be installed.
- ProductVersion, which specifies the version of the software to be installed.
- ProductCode, which specifies the globally unique identifier (GUID) that identifies the Windows Installer package.
- UpgradeCode, which specifies a GUID that Windows Installer uses to search for related versions of an installed product. Related products share the same UpgradeCode GUID.

The MSIInfo utility consists of two scripts: `MSIInfo.js`, which retrieves the five properties, and `MSIInfo-Context.js`, which adds a Windows Explorer context-menu option so that you can simply right-click an `.msi` file to display those properties. You don't need to adapt these scripts at all, which means you don't have to know how to read or edit a script to use them. I'll walk you through how to run them so you can get the MSIInfo utility working in your environment.

## Step 1

You first need to download the MSIInfo utility from the *Windows IT Pro* website. Go to [www.windowssitpro.com](http://www.windowssitpro.com), enter 103497 in the InstantDoc ID box, click Go, then click the 103497.zip link. Unzip the 103497.zip file, and place `MSIInfo.js` and `MSIInfo-Context.js` in the same folder.

## Step 2

The next step is to add the context-menu option to Windows Explorer by running `MSIInfo-Context.js`. Open Windows Explorer and navigate to the directory where you put the scripts. Right-click

Utility retrieves  
programs'  
names, versions,  
and more

by Bill Stewart

## ■ .MSI FILES

MSIInfo-Context.js, and choose Open (not Open with Command Prompt). MSIInfo-Context.js will display the prompt shown in Figure 1. Click Yes. The script then adds an option named Info to the context menu that appears when you right-click an .msi file in Windows Explorer. If you later want to remove that option, you simply run MSIInfo-Context.js again. When you're asked if you want to remove context menu support, click Yes.

Note that you need to run MSIInfo-Context.js under an administrator account or elevated permissions. Here are the specifics:

**Windows Server 2003, Windows XP, or Windows 2000.** If you're using Windows 2003, XP, or Win2K, you must run MSIInfo-Context.js under an administrator account.

**Windows Vista.** If you're using Vista and have User Account Control (UAC) enabled, you must use elevated permissions, even if you're logged on as an administrator. Here's why: When you're logged on as an administrator and you have UAC enabled, Windows disables the Administrators group token in your logon session. When you perform an action that requires privilege elevation, the OS prompts you for confirmation to enable the Administrators group token to prevent inadvertent changes to the system. However, this can make some administrative tasks more difficult, such as running a Windows Script Host (WSH) script (i.e., a .js, .vbs, or .wsf file) with elevated credentials.

Fortunately, there's a workaround for this problem. First, close any open Windows Explorer windows. Next, open Windows Explorer and choose Folder Options on the Tools menu. (If you can't see the Tools menu, press F10.) Then, select the View tab. Scroll down the list of advanced settings and enable the *Launch folder windows in a*

*separate process* option, then click OK. Close Windows Explorer.

Next, right-click a Windows Explorer shortcut (e.g., the one under All Programs, Accessories on the Start menu in Vista) and choose *Run as administrator* from the context menu. After confirming that you want to run Windows Explorer as an administrator, navigate to the folder containing MSIInfo-Context.js and run it. Since the Windows Explorer instance is running with administrator permissions, the script will run under those elevated permissions as well.

**Windows 7.** In Windows 7, it isn't possible to open an elevated Windows Explorer window when UAC is enabled, which appears to be due to a bug (see social .technet.microsoft.com/Forums/en-US/w7itprosecurity/thread/1798a1a7-bd2e-4e42-8e98-0bc715e7f641). If you're using Windows 7 and have UAC enabled, you need to run MSIInfo-Context.js under

## In Windows 7, it isn't possible to open an elevated Windows Explorer window when UAC is enabled.

elevated permissions using a Command Prompt window (i.e., cmd.exe). To do so, right-click a Command Prompt shortcut (e.g., the one under All Programs, Accessories on the Start menu in Windows 7) and select *Run as administrator* from the context menu. After confirming that you want to run cmd.exe as an administrator, enter the pathname of the script, enclosing it in double quotes (") if it contains spaces (e.g., "C:\Admin Scripts\MSIInfo-Context.js"), and press Enter. When MSIInfo-Context.js displays the prompt shown in Figure 1, click Yes.

**Windows Server 2008.** I don't have a Server 2008 machine for testing, but the steps for Windows 7 should work on Server 2008 as well.

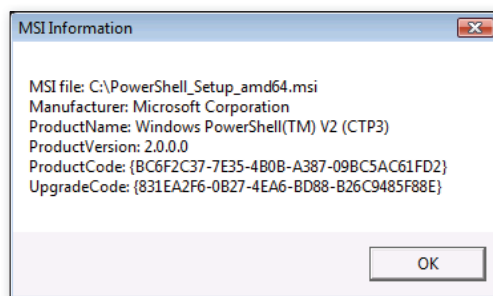


Figure 2: Sample results from the MSIInfo utility

### Step 3


The last step is running MSIInfo.js, which you don't need to run under an administrator account. All you need to do is navigate to the target .msi file in Windows Explorer, right-click that file, and select the Info option. MSIInfo.js will then run and display all five properties for that file in a message box, as Figure 2 shows.

Alternatively, you can run MSIInfo.js from a Command Prompt window. It uses the syntax

```
MSIInfo.js msifile [property]
```

You use the *msifile* parameter to specify the pathname of the .msi file you want to check. If the .msi file's pathname contains spaces, you need to enclose the parameter in double quotes. The *property* parameter is optional and must be one of the following case-sensitive property names: Manufacturer, ProductName, ProductVersion, ProductCode, or UpgradeCode. If you omit the property parameter, MSIInfo.js will display all five properties. If WScript is your default host in WSH, the properties will appear in a message box. If CScript is your default host, the properties will appear in the console window.

### A Few Clicks Is All It Takes

The next time you encounter an obscure .msi filename or need to find out the version of a software package that an .msi file will install, try the MSIInfo utility. With just a few clicks, you'll get the information you need. 

InstantDoc ID 103497

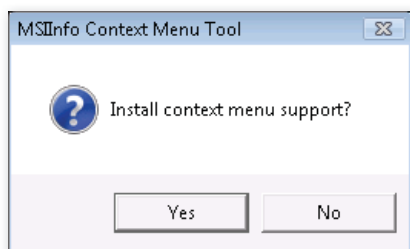


Figure 1: Adding the Info option



### Bill Stewart

(bill.stewart@frenchmortuary.com) is a scripting guru and the lead IT analyst for French Funeral and Cremation Services in Albuquerque, New Mexico.

# Make SQL Server Sing on Hyper-V

## Microsoft's virtualization solution comes into its own

In this article, we'll look at virtualizing Microsoft SQL Server in a Windows Server environment. Although Microsoft has offered virtualization products for the past several years, it's only been in the last generation of the Windows Server OS that Microsoft's virtualization solution, with Hyper-V, has come into its own. First we'll review the benefits of virtual servers, then we'll examine the unique challenges SQL Server presents when you attempt to run it on a virtual machine (VM). We'll explore how Windows Server 2008 Hyper-V is well suited to host SQL Server instances and the intelligent way upcoming SQL Server 2008 R2 takes advantage of a virtual environment.

### Benefits of Virtualization in Production

Before we begin discussing the benefits of virtualization, it might be best to start at the beginning. First there was a big bang—just kidding, not that far back. But we should at least explain what a VM is for those of you just joining the virtualization movement. Don't fret, we'll go deeper later in the article for you hard-core veterans.

In the simplest terms, virtualization is the practice of emulating a fully functioning server (known as a *guest OS*) via an application executing on the *host OS* of a physical server. The VM running the guest OS is delivered courtesy of a VM software application and can either be isolated, such as in a test or development environment, or be made available to the rest of the network as an independent server. Either way, fewer physical machines will be in the server room than the number of logical servers available to clients (see Figure 1).

Because a VM's guest OS can have applications installed and can provide network services to the rest of the network, a major benefit of virtualization in production is that a single physical server can serve multiple purposes on the network. Maintaining fewer robust physical servers, each providing multiple services, is more economical than supporting several physical servers, each dedicated to a single purpose.

By consolidating services and applications you can reduce ownership costs and power consumption while supporting a mix of physical and virtual network services within your environment. Centralized administration with the help of VM management utilities, such as Microsoft System Center Virtual Machine Manager (SCVMM), can reduce administration overhead while portable VMs lower the cost and downtime of disaster recovery, hardware migrations, and upgrades.

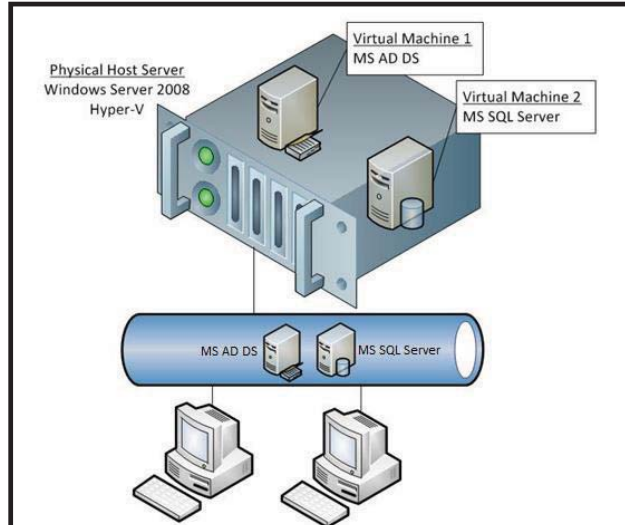


Figure 1: Virtual AD DS domain controller and SQL Server

### Optimal Hardware Utilization

With virtualization, multiple independent OSs can run simultaneously, each with its own access to the physical hardware. Imagine a VM guest OS and host OS, each taxing the CPU up to 25 percent concurrently and utilizing 50 percent of the CPU for a better rate of return on your chip investment. You can achieve higher yields on hardware investments with VMs, which can result in a lower total cost of ownership (TCO) for the network.

RAM is also heavily utilized in a virtualization solution when multiple OSs need memory space simultaneously. Server 2008 R2 Hyper-V employs an extra layer of memory address translation, which we'll discuss later in this article, to get the most out of the RAM chips. The I/O subsystem will also be well taxed by VMs that each require hard drive space to load their guest OS and applications. Server 2008 R2 Hyper-V offers a choice of virtual hard disk sizing to get the most use of local hard drives without endangering disk space.

You can leverage VMs to enhance availability of mission-critical applications and services. Each VM exists within a virtual disk file (which contains all the aspects of a physical disk, including sectors, file systems, files, boot records, and so on) so the entire guest OS can be ported from one host server to another. This portability makes it easy to recreate the server in both high-availability and disaster-recovery scenarios. We'll talk more about these concepts later in this article.

### Wendy Henry

(wendy@sharepointelearning.com) is a Microsoft Certified Trainer (MCT) who has been an independent technical trainer, author, and consultant for more than 10 years. She has specialized in Microsoft SQL Server since 1999 and SharePoint since 2005. Wendy is a contributing partner on SharePoint-eLearning.com and frequently teaches and presents at conferences on WSS 3.0 and MOSS 2007.



## Application Consolidation

Because virtualization provides OS isolation across common hardware resources, consolidating applications and services onto a specific server is possible. It has long been a Microsoft best practice to install resource-intensive server applications, such as SQL Server and Exchange, onto dedicated equipment. This best practice came into being because two beefy applications competing for the same resources (usually CPU and RAM) under the same OS roof would eventually cause a performance bottleneck.

But unlike loading both SQL Server and Exchange into the same OS, virtualization allows each application to be installed onto its own virtual server. Each application is unaware of the other application being on the same hardware. Obviously, concerns about making sure the host server has enough hardware resources to go around are valid, but the reduction in physical asset portfolio and cost—along with the opportunity to standardize best practices for all server applications—makes consolidation well worth the effort.

Server 2008 Hyper-V's native support for Microsoft applications eliminates additional hypervisor costs when setting up SQL Server in a virtual environment. Hyper-V is included with several editions of the OS. You can preconfigure each VM to a limited amount of RAM and hard drive space to prevent one particularly hungry guest OS from usurping more than its fair share of the hardware. You also can set standards for applications, and administrators can plan and govern SQL Server instance

configuration settings appropriately to operate within those boundaries.

## Consolidated Management and VM Portability

The IT requirements to manage multiple physical servers are less than the IT requirements to manage multiple virtual servers consolidated under a physical system. You have fewer hardware, space, and power considerations. Furthermore, VMs are portable and can be captured in various versions without the extraneous labor of an imaging solution often required to deploy or create a snapshot of a physical server's host OS and applications.

The Hyper-V console, which ships with Server 2008 R2, connects to individual VMs using RDP over TCP port 2179. But running multiple console windows into separate VMs is tedious when performing the same administration across multiple guest OSs.

A better idea is SCVMM 2008 R2 (see Figure 2), which consolidates all VMs into a single management utility and console. You can execute a single monitoring or configuration operation only once, yet target it to multiple VMs simultaneously. You can tailor the SCVMM UI to a user's preferences, facilitating smarter and faster server management. And here's the best news: SCVMM 2008 R2 connects to physical, virtual, and heterogeneous OSs to manage your entire network from one place.

Additionally, you can use System Center Operations Manager to monitor individual services across Microsoft, Linux, and UNIX platforms on both physical servers and VMs in a customizable single interface. And slated for release in early 2010, the

new System Center Service Manager 2010 will help enterprises enforce best practices, change control, and lifecycle management across all platforms in the network. You can employ these and more System Center solutions to centralize administration of large enterprises and reduce support costs.

Sometimes it might be necessary to move or copy a VM from one host OS to another; for example, during disaster recovery, new hardware migration, or high-availability initialization. And other times it might be beneficial to be able to create a point-in-time copy of a server to revert back to in case of detrimental software loads or configuration changes. Microsoft Hyper-V accommodates such endeavors with:

- Clones: Duplicate VMs generated via SCVMM (requires that the reference VM first have security identifiers removed by running the sysprep.exe utility)
- Snapshots: Point-in-time copies of a VM (disk, VM configuration, or both)
- Failover cluster support: Hyper-V is cluster aware and can run VMs on an active node of a Microsoft cluster
- Live Migration support: Uninterrupted rollover of a VM from one node of a Microsoft failover cluster to another node transparent to the client

For more information about combining failover clustering and Live Migration in Hyper-V, read the Microsoft TechNet article "Hyper-V: Using Hyper-V and Failover Clustering" at [technet.microsoft.com/en-us/library/cc732181\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732181(WS.10).aspx).

With all of these advantages, it's no surprise that virtualization of mission-critical resource-intensive network applications, such as SQL Server, has become so popular. And although some of these advantages beg further discussion, this article isn't a tutorial on the implementation of a VM but rather a look at optimizing SQL Server on a VM. So let's look at what makes SQL Server a good, or bad, candidate for virtualization.

## Unique Challenges to Virtualizing SQL Server

Like many of Microsoft's enterprise server applications, SQL Server demands deep hardware resources. But what makes SQL Server challenging is both its architecture

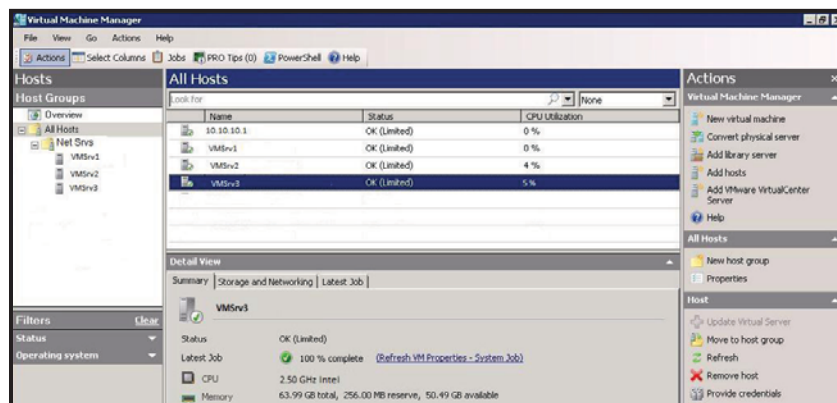


Figure 2: System Center Virtual Machine Manager console

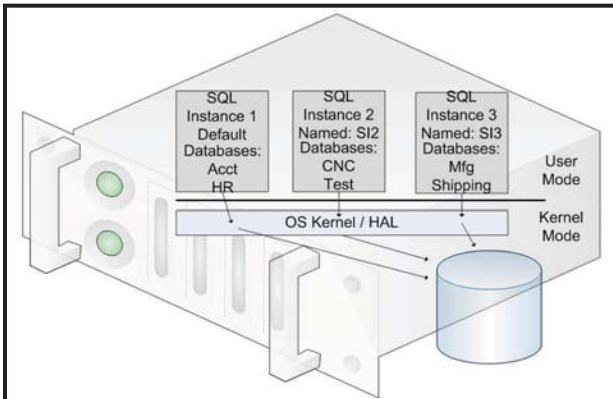


Figure 3: Multiple SQL Server instances

and its importance. Far more applications today are using SQL Server as their data repository, making SQL Server one of the most mission-critical applications on a network and often the subject of aggressive SLA objectives. Multiple SQL Server instances and SQL Server business intelligence (BI) solutions can influence VM design. And the critical nature of SQL Server databases often requires high-availability solutions such as database mirroring and failover clustering to ensure constant data availability to users.

**Multiple instances.** SQL Server has long had the capability to install multiple instances of the software onto a single OS (see Figure 3). Each instance employs its own SQL Server service, which means that processor overhead increases with each additional instance installed. Some registry information and even a service or two, such as the Distributed Transaction Coordinator service, are shared among all instances of SQL Server. But the two most industrious services of the relational database engine, MSSQLSERVER and SQLSERVERAGENT, are unique per instance. Multiple instances give administrators the opportunity to segregate sysadmin authority and programmers the chance to isolate their application databases apart from other data.

A downside of multiple instances is that they are subject to a single point of failure on a host OS. Corruption or a problem in the host OS could affect all instances running on the OS. An outage in a host OS could cause an outage in all the SQL Server instances.

Should you immediately embark on a project to consolidate all of your SQL Server databases into a single instance? No. Multiple instances maintain an administrative

boundary and in large enterprises with segregated IT departments, there may be different teams of SQL Server systems administrators (sysadmin role members) who should only have control over certain databases but not others. Separation of duties is a viable reason to continue

supporting multiple SQL Server instances. Another justification is the need for differing SQL Server instance-level objects and settings, such as throttle settings and native endpoint objects. But these arguments for multiple instances could also be satisfied by installing each instance on a separate VM (see Table 1).

#### Guest clustering vs. host clustering.

Another long-time challenge to supporting mission-critical SQL Server databases has been maintaining SLA commitments regarding data availability. Many software manufacturers, Microsoft included, rely on SQL Server databases as a data repository in their applications thanks, in part, to the product's value on the dollar (Express Edition is free). Furthermore, business information workers often rely on the family of BI products that ship with Standard, Enterprise, and Datacenter editions.

Keeping the data in a SQL Server database up and online all the time requires sophisticated high-availability solutions. Within the SQL Server and Windows OS

products, Microsoft offers several options for data redundancy, including:

- Database snapshot: Read-only point-in-time virtual copy of a database
- Log shipping: Latent transaction log copy process between two copies of a database
- Database mirroring: Synchronous or asynchronous transaction commitment to two copies of a database
- Replication: Snapshot, transactional, merge, or peer-to-peer data replication between two databases (granular to row or column level depending on article partitioning)
- Failover clustering: Failover clustering via Server 2008 R2 failover cluster to protect against OS or SQL Server service failures

Of these tools, clustering has become the front-running solution for providing immediate failover of a corrupt or incapacitated SQL Server instance (and thus all databases in it). Traditional host clustering, which is the art of implementing Microsoft cluster services on a Windows Server OS, is a popular topology. For more information about known issues with SQL Server 2005 installed on a Server 2008 failover cluster, see the Microsoft article "List of known issues when you install SQL Server 2005 on Windows Server 2008" at [support.microsoft.com/kb/936302](http://support.microsoft.com/kb/936302).

With the introduction of Hyper-V clustering technologies, the schematic of clustering has changed. The legacy idea of clustering multiple physical servers is now known as *host clustering*. Host clustering grants high availability to the host OS supporting a VM that has SQL Server installed, as well as the VM itself housing the SQL Server services.

Table 1:	Differences Between Multiple Instances and Multiple VMs Delivering One Instance Each	
Concern	Multiple Instances on One OS (Server 2008 R2 Enterprise/Datacenter)	Hyper-V Virtual Machines (single SQL Server instance each)
Processor	Up to 64 CPUs total for all instances Windows OS thread management SQL Server throttle settings	Up to 4 CPUs per VM Hyper-V thread management SQL Server throttle settings
RAM	Up to 2TB total for all instances Windows Virtual Memory Manager SQL Server throttle settings	Up to 64GB per VM Hyper-V SLAT memory management SQL Server throttle settings
I/O	Windows OS disk management	Hyper-V virtual disks (fixed, dynamic, or pass-through)
Autonomy	Process level (OS overhead)	Guest OS level (resource intensive)

Table 2:	Differences Between Host and Guest Clustering	
	Host Clusters	Guest Clusters
Nodes	Physical servers	Virtual machines
Service	Cluster feature in host OS	Cluster feature in guest OS translated by Hyper-V
Failover	Quorum managed	Quorum managed
Monitoring	Host and guest OS states	Guest OS and applications states

If something goes awry with the primary physical node (whether due to the host OS or VM), the services are brought online on the secondary node. Unfortunately, client connections will be interrupted during the migration and automatic reconnection. Shared SAN storage such as iSCSI, Fibre Channel, or Serial Attached SCSI (SAS) are ideal for host clustering topologies and can provide service level failover, if each VM is configured to use a virtual disk that maps to its own logical storage unit on the SAN.

Alternatively, you can use *guest clustering*, which clusters VMs inside the virtualization layer. In this design, the VMs themselves are clustered together as if they were independent physical servers. However, the state of both the guest OS and the applications running in it will be monitored and stored on the shared SAN storage of the guest cluster. Guest clustering allows failover of a single VM or single application within a VM in the event of VM failure through no fault of the host OS.

Key differences between host clusters and guest clusters are outlined in Table 2. In Figure 4, you'll see that host clustering between two physical nodes provides fault tolerance of all three VMs, whereas guest

clustering between VM1B-act and VM1B-pas is providing fault tolerance of the VM1B-act guest OS within the same physical server. Should the host clustering fail over, VMs VM2B-act and VM2B-pas would take on the guest clustering design.

Although guest failover clustering for SQL Server VMs is supported by Microsoft, you need to be running Server 2008. See the Microsoft article "Support policy for Microsoft SQL Server products that are running in a hardware virtualization environment" at [support.microsoft.com/kb/956893](http://support.microsoft.com/kb/956893).

**Database mirroring.** SQL Server 2008 offers a data duplication strategy called database mirroring. In essence, a database is backed up and restored to a separate SQL Server instance from the original. The two instances are connected through an instance-level TCP endpoint restricted to forwarding traffic for the purpose of database mirror activity only. As transactions are committed to the original database, they are also committed to the mirror through the endpoint (synchronously or asynchronously, depending on the mirror topology choice). The mirror database is offline to users until invoked during

a failover. Database mirroring is a fault-tolerance solution, not a load-balancing solution.

Mirroring can be supported between two VMs each running an instance of SQL Server. Whether the two VMs should reside on the same physical server or not depends on the level of protection being sought. If you're employing database mirroring strictly to protect from database or instance failure, the same physical server and host OS should be sufficient. If you also want to protect the database from physical device or storage failure, then separate physical servers would be necessary. When deciding, keep in mind that TCP/IP traffic between the SQL Server instances involved in the mirror design (and optional witness SQL Server instance) can be significant on a highly volatile database. Traffic between VMs on the same physical server never truly sees the light of day on the Ethernet network thanks to simulated network devices and Hyper-V translated drivers. Traffic between VMs on opposite physical servers will affect Ethernet network performance.

**BI and virtualization.** In recent versions, Microsoft has done an admirable job of adding functionality and purpose to the SQL Server product line. So much so, in fact, that many companies have begun to place a great deal of critical business data in the SQL Server Database Engine server application. But it doesn't stop there. The SQL Server family of products also boasts an impressive line-up of BI applications that can integrate heterogeneous data

platforms, automate routine data management tasks, construct data warehouses, and report on a myriad of data sources. These products include:

- SQL Server Integration Services (SSIS): Data extraction, transformation, and loading (ETL) solution
- SQL Server Analysis Services (SSAS): Data warehouse and mining solution

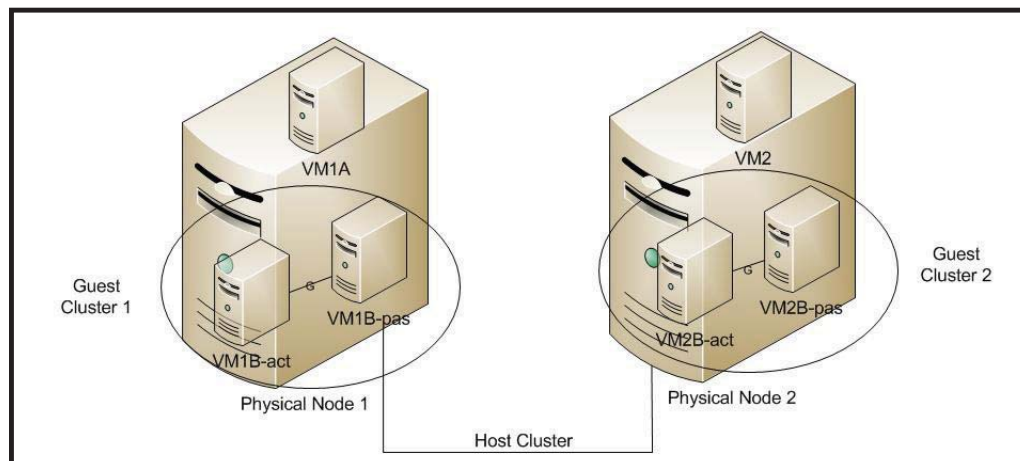


Figure 4: Host and guest clusters



- SQL Server Reporting Services (SSRS):  
Data reporting solution

Each of these BI subsystems is supplied with SQL Server Standard, Enterprise, and Datacenter editions, and Microsoft supports all of them to run in a virtualized environment.

**Running Hyper-V with SQL Server.** If your past experience in SQL Server virtualization is with Microsoft Virtual Server or Microsoft Virtual PC products, then you're in store for a treat. Microsoft Hyper-V is a step above these predecessor applications and has a completely different architecture primed for enterprise server applications. Better yet, it ships at no additional cost for Server 2008 R2 and is freely included in Server 2008 Hyper-V. Its native hypervisor eliminates the need for costly additional virtualization products when supporting Microsoft server applications. And its Integration Services can monitor both the host and guest OSs for health, time synchronization, registry key sharing, and graceful shutdowns.

**Processor loads.** Hyper-V on Server 2008 R2 supports up to 4 CPUs per VM and up to 384 VMs per host. Hyper-V multi-processor support for SQL Server 2008 lets SQL Server take advantage of multiple CPUs in the VM. Performance gains tend to diminish slightly when increasing from two to three processors or from three to four. Of course, each instance of SQL Server is unique and only testing and monitoring will reveal for certain the point of diminishing return when employing multiple processors. Variables such as the product involved (relational database engine versus BI), the number of concurrent sessions, and the nature of frequent actions can all influence CPU utilization. But Hyper-V's ability to simulate multiple processors in a VM is crucial to optimizing SQL Server performance.

Perhaps the biggest advantage Hyper-V has in supplying processor power to its VMs lies in its architecture. Unlike other virtualization applications, Hyper-V doesn't install on top of Server 2008 R2 in the User Mode layer. Rather, it lies beneath the OS as an abstraction layer, or micro kernel, to the hardware. This placement gives Hyper-V full management control over all hardware for

both the host OS calls and each VM guest OS. Although each VM is configured with a specific number of virtual processors, it's actually Hyper-V that determines which physical CPU core handles each request and how much time the request gets (including both host and guest OS requests).

Thanks to Hyper-V configuration settings (see Figure 5), administrators can dictate CPU allocations per VM by configuring virtual processors. This is both a blessing and a curse. While it's great to have such granular control over who handles each thread, without extensive knowledge and skills an administrator could inadvertently set the allocations too sparingly and underutilize physical processors while incapacitating CPU-hungry server applications running in the VMs. Hyper-V also supports virtual processors that don't map back to a single physical CPU or core to best accommodate server applications in a VM. And CPU Core Parking in Server 2008 R2 Hyper-V consolidates processes onto a minimal number of CPU cores, allowing idle cores to be suspended, or *parked*, to consume less energy.

For more information about monitoring performance of a Hyper-V VM, read the Microsoft whitepaper "Running SQL Server 2008 in a Hyper-V Environment—Best Practices and Performance Recommendations" at [download.microsoft.com/download/d/9/4/d948f981-926e-40fa-a026-5bfcf076d9b9/SQL2008inHyperV2008.docx](http://download.microsoft.com/download/d/9/4/d948f981-926e-40fa-a026-5bfcf076d9b9/SQL2008inHyperV2008.docx).

**Memory addressing.** In addition to managing processor cores, Hyper-V also manages physical RAM allocation. At creation time, a VM is configured to use a specific amount of memory space. Upon boot-up of the VM, the hypervisor reserves the configured space for that particular child partition (each VM is a child partition in Hyper-V) in physical RAM. Each guest OS can then use the issued memory space as if it is physical memory and offer virtual addresses to each application installed on the OS. These address spaces are known as:

- System Physical Address (SPA): Physical RAM address space of physical server hosting Hyper-V; uses paging file on physical disk to store overages

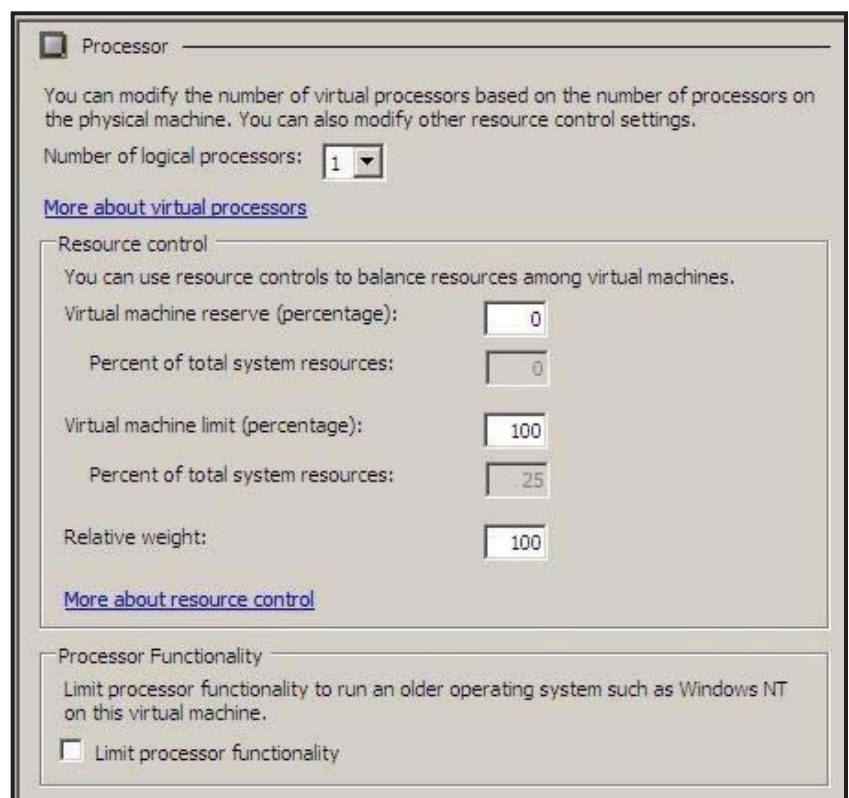


Figure 5: Processor settings for a VM in Hyper-V Manager

- Guest Physical Address (GPA): Allocated RAM address space allotted to a VM child partition
- Guest Virtual Address (GVA): Memory space greater than GPA allocated by guest OS to installed applications; uses paging file on virtual disk to store overages

In this design, Hyper-V must map memory twice—once from guest OS virtual memory addresses to the GPA address allocated to the VM child partition, then again from the GPA address to the SPA. Thus you have two opportunities for data in memory to become paged to the hard disk. Excessive paging becomes a performance bottleneck and can endanger the physical server's ability to support multiple VMs simultaneously. Because Hyper-V has knowledge of all allocated memory space, it can monitor physical RAM usage and prevent insufficient memory errors in the host OS.

Server 2008 R2 Hyper-V introduces a new technology called Second Level Address Translation (SLAT), wherein the hypervisor adds a second layer of paging to the architectural paging table of compliant CPU hardware. Because SLAT stores address translation information for both layers of virtual memory, the hypervisor doesn't need to retain information about the SPA-to-GPA mappings for multiple VMs on the server. This reduces overhead of Hyper-V while improving performance by maintaining translations at the hardware layer instead of with software. Memory-intensive applications running in VMs, such as SQL Server, benefit greatly from SLAT.

**Live Migration.** Being able to move an entire VM from one host to another is paramount to high availability, disaster recovery, and scalability. From updates to unexpected maintenance, occasions arise in which the VM must be relocated in order to continue servicing users. In Server 2008 R2, Cluster Shared Volumes allow multiple clustered VMs to use the same virtual storage (SAN logical storage unit) yet still be candidates for migration individually.

For more information about using Cluster Shared Volumes, see the Microsoft article "Overview of Cluster Shared Volumes" at [technet.microsoft.com/en-us/library/dd630633\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd630633(WS.10).aspx).

Live Migration leverages Server 2008 R2 failover clustering and the hypervisor to move a running VM from one node in the host cluster to another with no interruption to client sessions. The VM's files are stored in the shared storage of the Server 2008 R2 failover cluster (an iSCSI or Fibre Channel SAN), and each VM can simultaneously access those files. When a live migration is initiated, the VM memory from the first node is copied to the backup node. The VM is then started on the backup node, which can immediately access the VM files on the shared storage.

## SQL Server 2008 R2

Slated for release in May 2010, SQL Server 2008 R2 will further enhance SQL Server's support for Hyper-V. In this vein, SQL Server 2008 R2 is even friendlier toward clustering and virtualization than the current version of SQL Server.

**Clustering support.** SQL Server 2008 R2 introduces new cluster support for taking advantage of Server 2008 R2 failover clusters and Hyper-V guest clusters. Some examples of enhancements anticipated in R2 are:

- Clustered installs: Choice A = Integrated (1 node; additional nodes are added separately as needed) vs. Choice B = Advanced/Enterprise (all nodes are named during install and SQL Server binaries installed on each)
- Service accounts: R2 will support using service identifiers as opposed to domain user accounts for service accounts, thereby breaking dependency on authentication architecture
- Online node management: Nodes can be added/deleted from a cluster without interrupting services on the active node

**Virtualization.** A few enhancements in SQL Server 2008 R2 might influence your virtualization design. First, database mirroring will offer better transaction log compression during write-ahead synchronization. Also, a new lock hint in T-SQL allows programmers to disable lock escalation during specific statements. Databases maintained on separate instances across multiple VMs due to lock performance issues might soon be candidates for consolidation.

**Business intelligence.** BI is perhaps the most enhanced area of SQL Server 2008 R2. Although most of the changes are in client support, such as SharePoint integrated SSRS and self-service BI in Excel 2010, these enhancements will spur the implementation of BI solutions. As BI implementations proliferate in the enterprise, additional scalability will be important to support increased workloads and meet business SLAs.

## Installing SQL Server 2008 on Hyper-V

Installing SQL Server 2008 into a Hyper-V VM differs little from installing the application on a physical server's host OS. However, you should examine certain considerations before beginning the installation. Minimum OS requirements must be met by the guest OS chosen for the VM. In addition, the Hyper-V virtual disk type should be chosen carefully to best support SQL Server. Hyper-V offers three possible virtual disk structures:

- Fixed: Hard-coded with a set size, and that space is allocated on the physical disk for the .vhd file at VM creation. Despite the percentage used, the fixed .vhd file will always be the fixed size.
- Dynamic: Initial .vhd size grows as the data stored grows. This structure makes efficient use of the disk initially but is vulnerable to insufficient free space due to other demands on the hard drive.
- Pass-through: VMs write directly to storage. This is the optimal storage strategy for SQL Server because many SAN platforms offer LUN administration that can stretch a single LUN across multiple physical spindles and replicate data for fault tolerance and high availability.

The bottom line is that production SQL Server 2008 instances are prime candidates for running in a VM, and Server 2008 R2 Hyper-V is the best virtualization application Microsoft has produced to date for supporting mission-critical, resource-intensive server applications such as SQL Server. This article introduces the key concepts and will hopefully whet your appetite to learn more about these powerful tools.



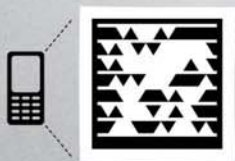
InstantDoc ID 103658



Efficiency you can feel,  
but can't touch.


Finally, a consolidated virtualized infrastructure, from the data center to the desktop, is within grasp. Well, not literally of course. After all, it's virtualized. Start with Windows Server® 2008 R2 with built-in Hyper-V™ and you can eliminate costly third-party software like VMware. Add SQL Server® 2008 Enterprise, with unlimited virtualization, and you just made it easier to eliminate racks of underutilized servers. Toss in System Center and you've centralized management across the enterprise all the way down to the application level. Translation? Flexible and dynamic virtualized infrastructures that help maximize ROI, reduce TCO and improve business continuity. Just don't let the efficiency go to your head.

To learn more about how server virtualization can make you more efficient, go to [itseverybodysbusiness.com/virtual](http://itseverybodysbusiness.com/virtual)



Snap this tag to get the latest news on server virtualization or text VIRTUAL to 21710

Get the free app for your phone at <http://gettag.mobi>

Because it's everybody's  business



## NEW &amp; IMPROVED

■ Backup & Recovery  
■ Security

■ Log Management  
■ SharePoint

### Deduplication Appliance Builds a Greener Infrastructure

Nexsan has announced **DeDupe SG 2.0**. DeDupe SG 2.0 is the first LAN-based deduplication appliance that provides continuous data access and automatic backup application failover. According to the vendor, the appliance offers backup server connections of up to 5.4 terabytes per hour and support for Symantec OST. DeDupe SG 2.0 uses Nexsan's AutoMAID technology to place disk drives into their most energy-efficient state, making it more power efficient than competing solutions. Features in the latest version include: redundancy appliances for high availability;



## PRODUCT SPOTLIGHT

### NitroSecurity Offers Integrated SIEM/Log Management System

NitroSecurity has announced version 8.4 of **NitroView Enterprise Security Manager (ESM)** and **Enterprise Log Manager (ELM)** to provide a comprehensive log and Security Information and Event Management (SIEM) solution. According to the vendor, the tight integration between these two systems allows enterprises to lower the costs for many security and compliance operations.

"Ever-expanding regulatory requirements and compliance timeframes—from PCI, to HIPAA, to NERC—continue to widen the gap between log management and security information functions like behavior analysis and forensics," notes a vendor press release. "Unlike SIEM 'suites' from other vendors, the full integration of NitroView ELM takes advantage of the highest performing SIEM engine on the market. It allows organizations to greatly improve IT security efficiencies and strengthens regulatory compliance while reducing

post-event analysis and forensics from hours to seconds."

NitroView ESM includes geo-location tracking, providing a visual representation of where external activities (such as user/application traffic or security attacks aimed at systems) are geographically concentrated. Once NitroView ESM detects a problem, it more easily points the user to a source log file.

"As the latest version of the industry's first and only content-aware SIEM, NitroView V8.4 drills deep and monitors all traffic on the network up to the application layer, protocol use and individual sessions. Using patented data storage and management technology that smashes performance barriers plaguing other SIEM providers, NitroView is able to collect and manage billions of events, logs, network activity flows, and even application content—while maintaining the real-time analytics that are required for rapid incident response," reads the press release. To learn more, visit [www.nitrosecurity.com](http://www.nitrosecurity.com).

automatic backup; replication support for up to 150 remote sites; optional 10-Gigabit Ethernet connections (10 GbE); and others. To learn more, visit [www.nexsan.com](http://www.nexsan.com).

### SAFENTRIX Launches Free Outbound Email Security Service

SAFENTRIX announces **SAFENTRIX**, a cloud-based hosted email security service that provides spam and virus filtering for incoming and outgoing emails. Features include seven-layer spam protection, virus protection, near-zero false positives, malware and phishing protection, and support for up to 20,000 users per domain. The base service is free, making it a viable solution for small businesses. There is also a premium, paid service available. To learn more, visit [www.safentrix.com](http://www.safentrix.com).

### Laserfiche and FileTek Partner To Bring Email Management System

Laserfiche and FileTek have announced **Trusted Edge Intelligent Email Archive for Laserfiche**, a solution that enables secure, enterprise-wide email management and eDiscovery compliance. Features of the system include: Microsoft Outlook/OWA and Lotus Notes integration for transparent mailbox management; .pst file archiving; message classification, tagging, and annotation; file server and SharePoint intelligent archiving capabilities; and full audit and

NEW & IMPROVED

## Paul's Picks

www.winsupersite.com



**SUMMARIES** of in-depth product reviews on Paul Thurrott's SuperSite for Windows

### Windows Activation Technologies Update for Windows 7

**PROS:** Optional update

**CONS:** Unnecessary complexity due to Microsoft's invasive antipiracy technologies

**RATING:** ♦♦♦♦♦

**RECOMMENDATION:** Windows Activation Technologies Update (WATU) for Windows 7 is available worldwide via Windows Update and as a download from Microsoft's Windows Genuine website. As with a similar update that the company supplied with Windows Vista SP1, WATU is designed to address attempts to bypass product activation (over 70 kinds of attempts, in fact). According to Microsoft, these attempts have grown more sophisticated and, perhaps more alarming, some come with malware as well. WATU offers new "phone home" behavior: It checks every 90 days for new antipiracy updates. I see this update as largely innocuous, unless you're a software pirate—or victim of piracy.

**CONTACT:** Microsoft • www.microsoft.com

**DISCUSSION:** www.winsupersite.com/win7/watu.asp

### Apple iPad

**PROS:** Proven platform that works well on a larger form factor; compatible with iPhone apps

**CONS:** No one asked for a device that sits between a smart phone and a PC; it doesn't run Windows; Apple hasn't proven it can handle so many different products well

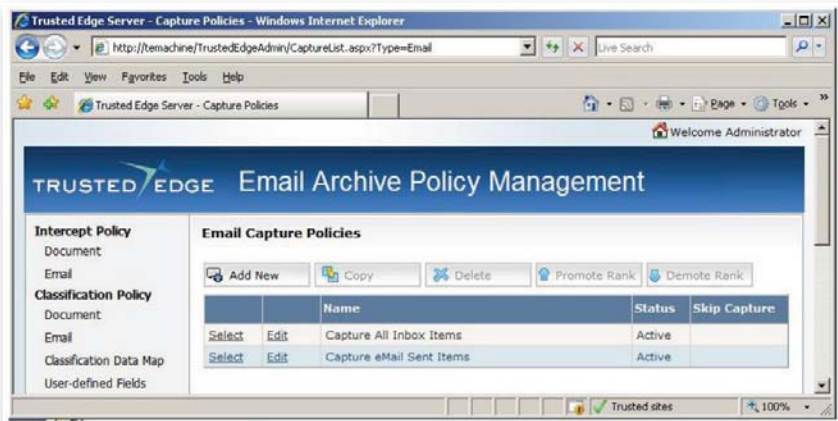
**RATING:** ♦♦♦♦♦

**RECOMMENDATION:** Apple's iPad is a 10-inch non-widescreen tablet device that runs a new version of the iPhone OS, is compatible with iPhone OS applications, and runs its own applications too. The device is sold in a dizzying array of versions, some with pay-as-you-go 3G wireless, some without, and with memory allotments of 16GB to 64GB. The iPad should shine in so-called casual computing environments, for tasks like browsing the web. But because it doesn't run a real desktop, it isn't compatible with any of the apps that people use every day. Apple says it's trying to jumpstart a new product category. Although I would argue that this category is new only to Apple, it's never wise to bet against Apple. I think you should wait: The company will almost certainly lower prices, simplify the product matrix, and ship more functionality.

**CONTACT:** Apple • www.apple.com

**DISCUSSION:** www.winsupersite.com/alt/ipad\_preview.asp

InstantDoc ID 103634



reporting. The platform also provides template archive policies for easy, out-of-the-box deployment. To learn more, visit [www.laserfiche.com](http://www.laserfiche.com) or [www.filetek.com](http://www.filetek.com).

### Zeacom Expands Capabilities of Office Communications Server

Zeacom introduced the **Zeacom Gateway for Microsoft Office Communications Server** (OCS), offering integration between Zeacom's unified communications technology and OCS. Unified communications continues to gain traction in enterprises as an efficient system for bridging email and telephony systems. With Zeacom Gateway, for instance, a customer service representative could make a call at the click of a button while within Microsoft Outlook. To learn more about how the system works, visit [www.zeacom.com](http://www.zeacom.com).

### SecretWeapon Systems Releases Image Capture Application

SecretWeapon Systems released a free windows OS image capture software called **SecretWeapon Image Manger**. SWIM lets you capture, restore, and apply OS images, as well as partition hard drives. According to the vendor, SWIM builds on the capabilities of Microsoft's ImageX by

offering an intuitive GUI to make image capture easier. To download the program, visit [www.getasecretweapon.com](http://www.getasecretweapon.com).

### 5280 Solutions Releases New SharePoint-based Records Management Solution

5280 Solutions announced the release of **Dynamic RM**, a SharePoint-based records management solution designed to manage electronic and physical records. Dynamic RM offers file plan visualization, declaration and preservation, flexible retention rules, and formal hold and consigned disposition processing workflow—in other words, it lets you apply traditional record-keeping practices in a SharePoint interface. With increasing regulatory pressure and the cumbersome nature of large paper archives, a web-based records management solution has a strong appeal. To learn more, visit [www.5280solutions.com](http://www.5280solutions.com).



# Automation Anywhere 5.5 Enterprise

Automating routine IT tasks has taken on new urgency as staff levels drop and resources dwindle. If you've wished you had time to write a program to do a routine task for you, you'll like the premise behind **Automation Anywhere**. AA lets you build scripts that perform repetitive tasks without writing code. Instead, you either pantomime your task or create a step-by-step procedure using AA's point-and-click task builder. AA has several versions, ranging from the entry-level Automation Anywhere Standard edition through the multi-user Server edition. This review looks at the midrange Enterprise edition, which lets you create and distribute automation packages to other users even if they don't have AA installed.

AA can automate a wide range of chores, from basic Windows configuration steps, through scripting desktop applications such as Microsoft Excel and Word, to the ultimate: remote database and networking processes. You can access and interact with web pages, securely copy files via SFTP, and deploy tasks without an agent to other computers in a domain. Tasks can be scheduled for repeated execution, integrated into a workflow comprised of multiple tasks, or saved as a stand-alone .exe file, executable on any Windows box without any additional software.

AA can automate a wide range of chores, from basic Windows configuration steps, through scripting desktop applications such as Microsoft Excel and Word, to the ultimate: remote database and networking processes. You can access and interact with web pages, securely copy files via SFTP, and deploy tasks without an agent to other computers in a domain. Tasks can be scheduled for repeated execution, integrated into a workflow comprised of multiple tasks, or saved as a stand-alone .exe file, executable on any Windows box without any additional software.

The core of AA is Task Editor, which you can open directly to begin composing a task script, or indirectly via AA's Watch mode. Here you perform the chore you want to automate while AA records the steps and builds a script for you. AA sports hundreds of standardized task actions, such as running an Excel macro or executing a SQL query, or you can create your own. While building a script, you can execute steps incrementally, which greatly simplifies task streamlining. Also during editing, a visualization feature lets you flag individual steps with a Snap Point icon, which captures a storyboard of screenshots of the script at those points when you run it in development mode. This is a terrific feature for documenting the steps a script performs. Alas, you can't save Snap Points in the Enterprise edition; only the Server edition has that capability. And you can't print

the storyboard, which limits its usefulness.

AA includes a few dozen pre-built task templates that automate common tasks, such as website data extraction and scheduled file transfers. You can purchase an optional Integration Pack with advanced functions, such as optical character recognition (OCR) and the ability to integrate with Java, to integrate with a wider range of external applications.

One level up from the Task Editor is AA's Workflow Designer, which Figure 1 shows. It lets you assemble multiple tasks into a series, with alternate paths available should a step fail or other conditions occur. Although Workflow Designer's capabilities are rudimentary (it doesn't support variables or iterations, for example), it's useful for automating processes consisting of multiple tasks.

Alongside Workflow Designer is Report Designer, which lets you generate and print reports showing the execution history of tasks over time. A return-on-investment (ROI) calculator lets you assign financial values to tasks and compute the savings achieved through automation. However, Report Designer can't print the scripts contained in a task, or the storyboard created by Snap Points, although you can export scripts as plain text files one at a time.

Two other wizards round out AA's feature set. Deployment Designer lets you select an individual task (but not a workflow) for deployment to a list of machines in the Windows domain, with flexible scheduling and runtime options. Trigger Manager can execute tasks or workflows based on external events, such as a folder or file change, a service or process starting or stopping, or various

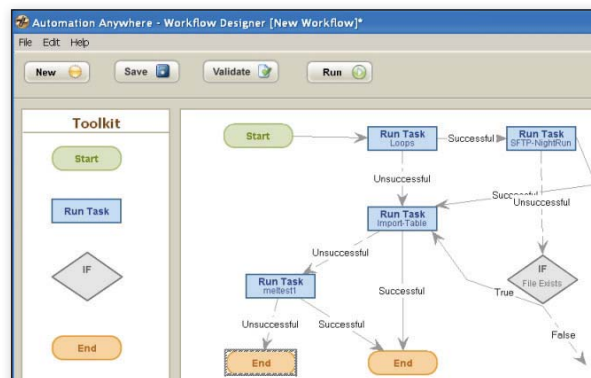


Figure 1: Workflow Designer

system performance changes, such as disk space or CPU consumption.

Despite a robust feature set, AA has room for improvement. Its inability to print scripts or storyboards is surprising in a product costing \$2,500.

Automation Anywhere Enterprise is a powerful tool that can simplify life for IT across multiple realms. In particular, the ability to encapsulate tasks and send them to users via email or web download is a boon to Help-desk administrators.

InstantDoc ID 103610

## Automation Anywhere 5.5 Enterprise

**PROS:** Huge range of task widgets; can save tasks as .exe files and run on any Windows machine; storyboard feature documents scripts with screenshots

**CONS:** Can't save Snap Points; no script or storyboard printing

**RATING:**

**PRICE:** \$2,495; \$3,490 with Integration Pack

**RECOMMENDATION:** Automation Anywhere Enterprise is a full-featured, multi-environment workflow automation tool with an extensive set of task templates. It can automate web and network tasks, database manipulations, testing, and data collection processes, as well as desktop applications such as Microsoft Excel. It's a powerful tool that can simplify life for IT across multiple realms.

**CONTACT:** Automation Anywhere • 888-484-3535 • [www.automationanywhere.com](http://www.automationanywhere.com)



Mel Beckman | [mbeckman@penton.com](mailto:mbeckman@penton.com)



# WMIX 2.0

In our early attempts to complete the work of 10 admins in the life of one, we first turn to the immutably useful utilities of old. The tacit need to automate these utilities soon pushes us to learn scripting, which, in turn, creates a need to abstract system properties at a high level. Windows Management Instrumentation (WMI) is Microsoft's answer to this need. However, accessing and using WMI can be complicated, especially for those of us who aren't interested in becoming programmers. Fortunately, PJ Technologies offers **WMIX 2.0**, a GUI-based implementation of this technology. It targets admins who want the customizability of a homespun script with the ease of use proffered by a graphical interface.

Installing WMIX 2.0, which runs on Windows 2000 and later, is straightforward. It opens with a clean interface that presents you with a favorites list, a WMI browsing tree, and a tidy toolbar that gives you access to the script and report generation wizards (see Figure 1). Besides letting you manually select computers to query, the favorites list can grab computers from Active Directory (AD) containers or by scanning IP blocks. Once the computers are selected, you can add them to the tabbed WMI browsing window or run queries directly against them via the context menu. No special permissions are required until you begin performing queries on remote machines, at which point WMI has its own set of assignable permissions accessible from the WMI management console (wmimgmt.msc).

After populating the browsing window, you can begin to dig into WMI to get a better idea of its breadth. From Windows Product Activation (WPA) to command-line environment variables to connected disks and network adapters, the vast majority of remote monitoring and administrative features are exposed through WMI. Many of these objects already have built-in scripts attached to them, such as a set of scripts for enumerating and deleting registry keys. If you want to, say, change a network setting using one of these scripts, you'd export the script, at which point you can modify (if needed), test, and deploy it.

VBScript is still the primary language by which WMI is accessed, so that's the

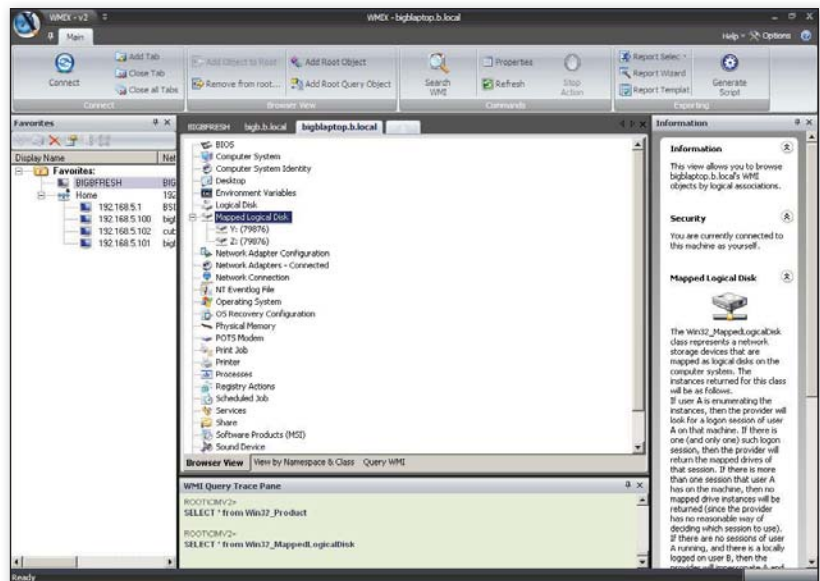


Figure 1: WMIX's interface

scripting language used by WMIX. VBScript runs via Windows Script Host (WSH), which has been included and installed with every version of Windows since Windows 98. Unfortunately, WMIX 2.0 doesn't support PowerShell. While this isn't a serious omission at the moment, many people are moving to PowerShell, so I hope to see it supported in the next release.

Another improvement I'd like to see concerns the export function. It feels a bit rushed, given that it merely generates your script and dumps it into a Notepad document. I'd like to see a basic built-in editor to round out the experience. If done right, this would make WMIX feel more complete. As I see it, admins could then edit scripts and learn using the resources of WMIX's search functions without continually needing to switch in and out of the program.

Scripts aren't all that WMIX outputs. You can easily generate and run one-off queries, which can be useful for troubleshooting. You can also create HTML-based inventory reports. It has never been easier to fire a data-backed response back to your boss that, for example, lists all of your computers that are already WPA activated and running version 12.x of your email client.

The more veteran WMI spelunker will be happy to know that WMIX has the ability to query WMI directly in addition to searching

and browsing its information store by namespace and class. These capabilities make lighter work out of script development and modification for those with experience writing scripts. In addition, said scripter can use WMIX to create WMI Group Policy filters that permit dynamic, targeted deployment of policies based on WMI attributes.

No matter your background, if you plan on exploiting WMI to the fullest (and you should), WMIX is a steal at only \$89 per license. It's a shoe-in given that it provides raw access to the API that powers far more expensive tools and it doesn't require a steep learning curve to use. If you want to get into WMI, then X marks the spot.



InstantDoc ID 103579

## WMIX 2.0

**PROS:** Simple, polished interface; makes the power of WMI accessible to everyone; provides agentless inventorying and administration; can build WMI Group Policy filters

**CONS:** Export function could use some enhancement; PowerShell not supported

**RATING:** 

**PRICE:** \$89 per license

**RECOMMENDATION:** WMIX does an excellent job exposing the inner workings of WMI, letting admins easily create custom-tailored management scripts while remaining easy on the IT budget.

**CONTACT:** PJ Technologies • 888-330-4188 or 786-268-3517 • [www.pjtec.com](http://www.pjtec.com)



Brandon Carse | [bcbigb@gmail.com](mailto:bcbigb@gmail.com)

IT pros are constantly bombarded with information—we face a labyrinth of event data in the form of firewall, server, router, switch, and other log files every day. When something goes wrong, we must descend into that labyrinth, seeking the root cause of the problem. **Splunk 4.0** collects, sorts, and correlates all that event data for you ahead of time, making your log file explorations faster and easier.

This product parses any and all types of log files or diagnostic output streams using an intelligent regular expression (regex) engine, and then it makes the output searchable from a web interface. Splunk input includes message queues, Windows event logs, registry hives, packet captures, intrusion detection alerts, UNIX syslogs, web access logs, Netflow streams, and more. Splunk parses timestamps and information fields for each source before indexing all of it in a searchable database. If Splunk makes a minor error, you can correct it by training its parsing engine using the built-in data input control panels. For more complicated inputs, you can use the configuration files, which allow for custom regex definitions.

Splunk requires a database server, which will handle data input processing and search queries on that data, at each data hub. It offers a comfortable, quick web interface that delivers simple yet powerful search-augmentation tools laid out in a straightforward workflow.

Splunk's query engine uses typeahead, search history, and its knowledge of parsed fields to help you construct a meaningful, accurate search. Key to the process, however, is the iterative addition of search terms that refine your results. These iterations leverage booleans, wildcards, and extracted fields to help narrow your data set. Events pop up that are physically near, and usually related to, the incident in question. Once you've determined the time frame for the problem, the key advantage of universal timestamping becomes apparent. This contextual vantage point gives you the ability to trace more complicated interactions back to their source, as Figure 1 shows.

**spunk> Search**

Summary Search Status Views Searches & Reports Help About

Search | Actions

source="VM1:LocalNetwork" Custom

22,500 matching events

Timeline: zoom in zoom out select all Scale: linear log 1 bar = 1 hour

Dec 15, 2009 03:00

1500 events at 8 AM on Tuesday, December 15, 2009

Dec 16, 2009

21 hours

22,500 events from 3:00:00 AM December 15 to 12:00:00 AM December 16, 2009

Selected fields (3): host (1) source (1) sourcetype (1)

Other interesting fields (12): BytesReceivedPerSec (n) (28) BytesSentPerSec (n) (27) BytesTotalPerSec (n) (32) CurrentBandwidth (n) (3) index (1) InetOut (n) (2) Name (5)

1 12/15/09 20091215212829.000000 BytesReceivedPerSec=0 BytesSentPerSec=0 BytesTotalPerSec=0 CurrentBandwidth=1000000 Name=HS TCP Loopback Interface wmi\_type=LocalNetwork host=Dig0 - sourcetype=VM1:LocalNetwork - source=VM1:LocalNetwork

2 12/15/09 9:28:29:000 PM 20091215212829.000000 BytesReceivedPerSec=0 BytesSentPerSec=0 BytesTotalPerSec=0 CurrentBandwidth=1000000 Name=Kaschi Network Interface wmi\_type=LocalNetwork

Results per page

Figure 1: An iterative search in progress

an unlimited amount of data per day, albeit at the hefty price of \$5,000. After investigating Splunk alternatives, I found that Splunk Enterprise's price isn't as exorbitant as I first thought, given the product's target markets and the fact that its feature set appears to be more complete and cohesive than those of its competitors. Nonetheless, I do wish there were a price point tailored for data-rich small-to-mid-sized businesses (SMBs).

The Enterprise edition offers role-based access controls and enterprise dashboards, which let users share useful searches and reports with their team. The crown jewel of the Enterprise edition is its distributed searches, which are bolstered by load-balancing and failover mechanisms. Splunk Enterprise also lets you architect data flows from your data hubs (called “forwarders” in this role) so that they feed indexed data up a hierarchy at regular intervals. And the Enterprise edition offers sophisticated monitoring and alerting functionality.

Despite its power, Splunk's interface has a few small cracks. There were some interface bugs, which were likely a result of the intricacies of maintaining a consistent experience on multiple web browsers and their associated OSs. These issues are primarily cosmetic, and rarely affect typical use, but they do underscore the importance of sticking to

clean browser installs to reduce conflicts with Splunk's otherwise slick interface.

Splunk pulls together disparate reports and unifies them in a clean, searchable manner. Although its pricing scheme could use a tier for SMBs, the product can still help you manage at least the core fraction of your IT data files. If you're stuck in a virtual cell padded with the remains of unused or unusable records and log data, Splunk will help restore your sanity.

InstantDoc ID 103481

## Splunk 4.0

**PROS:** Sophisticated event correlation and analysis across a variety of log file formats; refinable search results with Boolean expressions and typeahead; clean, fast web interface; free version; supports multiple platforms

**CONS:** Splunk Free is limited to 500MB per day; pricing for Splunk Enterprise is aimed at data centers and medium-to-large businesses, leaving a gap for SMBs; some minor runtime glitches

**RATING:** 

**PRICE:** \$5,000 for Splunk Enterprise; no charge for Splunk Free

**RECOMMENDATION:** Pricing aside, Splunk has excellent potential to help you manage data collection and restore logging data to its former usefulness.

**CONTACT:** Splunk • 415-848-8400 • [www.splunk.com](http://www.splunk.com)



Brandon Carse | [bcbiqb@gmail.com](mailto:bcbiqb@gmail.com)

# 2 Tools to Restore Active Directory Objects

Even the best-run network might need one of these solutions

Eric B. Rux

Remember when Windows 95 introduced us to the Recycle Bin? We've had this feature for so long, we forget how painful it was in the olden days—until we accidentally delete something in Active Directory (AD). Windows Server 2003 introduced the concept of the AD Recycle Bin. Unfortunately, nobody in Redmond wrote a GUI for the new feature. This led to a couple of free tools that tapped into the deleted objects, letting you save the day (and, perhaps, your job). One notable entry was Mark Russinovich's AdRestore, a small, 42KB tool that allows you to recover deleted AD objects (see more about this tool and two others in the sidebar "3 Free Active Directory Restore Solutions"). Unfortunately, only the object itself is recovered with these tools; individual attributes aren't.

Windows Server 2008 R2 improved on the original AD Recycle Bin, but it still doesn't come close to the feature set of the two products in this review. Before I dive into the features of these two products, I'd like to point out that under best circumstances, incidents like accidental object deletion shouldn't happen. A properly designed organizational unit (OU) structure with delegated security permissions prevents desktop technicians and junior administrators from deleting AD objects in the first place (they should have permission to disable, but not delete).

However, even the best-run network still needs to ensure survival in the case of an "oops" or in case of a disaster. Let's check out how these two products can help you in this endeavor. One is an inexpensive, very useful "Chevy" and the other is a much more expensive "Cadillac."

## NetWrix Active Directory Change Reporter

NetWrix Active Directory Change Reporter lets you quickly restore deleted or modified objects in any version of AD (Windows 2000 Server or later). It also includes a robust reporting feature that keeps track of all AD changes that occurred in the last 24 hours.

Setup is with a simple 8MB file after the prerequisites (IIS and .NET 2.0) are installed. After you accept the license agreement and select the file

location, installation takes only a few seconds. When the installation is complete, a dialog box asks you to either configure the application later, launch a basic configuration, or launch a full-featured configuration. I decided to use the basic configuration that the Quick Start Guide recommends.

After I entered the license information, I used the Quick Start Guide to configure the remaining settings, such as long-term archiving of deleted AD objects, SMTP server, and the email accounts where the AD reports should be sent. This wizard also walks you through setting up advanced reporting (SQL Server Reporting Services), and a report delivery schedule. Licensing is set via a serial key code.

A dialog box informed me that the tombstone lifetime property was set to 180 days and advised that I change it to 744 so that deleted objects could be recovered. To do so, I could choose Yes in the dialog box.

After the simple installation was complete, I naturally tried to delete something to see if I could recover it. I created a new user called "Eric," then promptly deleted it. Next, as Figure 1 shows,



Figure 1: The NetWrix AD Object Restore Wizard



## ■ ACTIVE DIRECTORY OBJECTS

### 3 Free Active Directory Restore Solutions

Still want to tap into the tombstone recycle bin found in Windows Server 2003 and later but don't need additional features? Try a freeware solution. It's probable that there are more than the three free solutions I list below—please drop me a line and let me know. I'll keep the online version of this article updated with any additional products that I hear about. If you didn't know about the Active Directory Recycle Bin or these tools, fire up your VM lab and give these a try. For free utilities, they're pretty cool.

**AdRestore v1.1.** This is a Microsoft solution written by Mark Russinovich. Find it at [technet.microsoft.com/en-us/sysinternals/bb963906.aspx](http://technet.microsoft.com/en-us/sysinternals/bb963906.aspx). As you might recall, Mark has written many, many useful freeware utilities such as psexec, regmon, filemon, and of course, the famous BSOD screensaver. The lightweight AdRestore command-line utility is simple to use: Execute "adrestore.exe" to see the objects that are available to recover, then run "adrestore.exe /r" to recover an object. Simple, and effective.

**Quest Software Object Restore for Active Directory.** This product is very similar in functionality to Mark's AdRestore but has a GUI interface that might be more comfortable for some administrators. Find it at [www.quest.com/object-restore-for-active-directory](http://www.quest.com/object-restore-for-active-directory). In my tests of both products, their functionality appeared to be identical.

**Quest Software Active Directory Recycle Bin PowerPack.** This tool extends Quest's PowerGUI admin console. Find it at [www.powergui.org/entry.jspa?externalID=2461&categoryID=21](http://www.powergui.org/entry.jspa?externalID=2461&categoryID=21). The first step is to download both the PowerPack and PowerGUI. Install PowerGUI, then import the PowerPack. What I really like about this tool is that it checks to see if the Windows Server 2008 R2 Recycle Bin feature is turned on, then offers to turn it on for you. Note that this action is irreversible and involves more than a simple click—be sure to do your due diligence before turning this feature on. More details can be found at [technet.microsoft.com/en-us/library/dd391916\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd391916(WS.10).aspx).

I chose the NetWrix AD Object Restore Wizard, which quickly walked me through restoring my object. However, just like in some freeware AD restore tools, such as the AdRestore utility, only the object itself is restored—the properties (last name, description, office) and any group memberships aren't recovered.

To restore the whole object (including the individual properties within the object), you need to take a snapshot of the directory ahead of time. This is done on a schedule for you every 24 hours or you can run it manually via Windows Scheduled Tasks. With this snapshot, you can restore not only the object but all of the attributes within the object.

NetWrix also has a very sophisticated reporting feature that tracks what happens to objects in AD. Some examples of reports you can choose include *All AD Changes by Date*, *All AD Changes by Object Type*, and *All AD Changes by User*. There are 38 pre-canned reports that offer a view into AD that many admins desperately need. In addition, another 33 reports track changes to Microsoft Exchange Server and Group

Policy. If these reports don't provide the information that you require, you can use SQL Server Reporting Services to dive deeper into the data. Note that Win2K doesn't track the "Who Changed" field in AD. If your AD domain is set to Win2K functionality level, not having this information recorded will affect you.

Netwrix AD Object Restore has an impressive feature set for a small price point. If you need something better than the built-in functionality that Microsoft delivers, yet don't want to pay the price of the big boys, then AD Object Restore is the obvious choice.

### NetWrix Active Directory Change Reporter

**PROS:** Simple, inexpensive "oops" protection that's one step above the free utilities; impressive canned reports show you what's going on inside your AD domain.

**CONS:** Not designed for complete AD recovery

**RATING:** ◆◆◆◆◆

**PRICE:** \$3 to \$4.50 (depending on user count); AD Object Restore version (no reporting) also available for \$1.00 to \$1.50 (depending on user

count) as well as a feature-limited freeware version.

**RECOMMENDATION:** If you need AD reporting and want better protection than the freeware products provide but don't have a lot of coin, NetWrix should be your first stop in your product search.

**CONTACT:** NetWrix • 888-638-9749 • [www.netwrix.com](http://www.netwrix.com)

### Quest Recovery Manager for Active Directory

Quest Recovery Manager for Active Directory is an enterprise-level directory services recovery tool. In addition to providing tombstone and rollback functionality, Recovery Manager can also restore entire domain controllers (DCs)—even to dissimilar hardware.

The setup for Recovery Manager takes significantly longer and is more involved than the NetWrix product and requires quite a few prerequisites: Microsoft SQL Server 2008 Native Client, Microsoft .NET Framework 3.5 SP1, SQL Server Compact 3.5 SP1, SQL Server System CLR Types, SQL Server 2008 Management Objects, and Windows PowerShell 1.0. Each prerequisite is included and is installed for you. The setup requires one reboot halfway through the installation, but it immediately continues where it left off. A license file provides product licenses.

The longer setup time for Recovery Manager merely reflects the fact that it's a much larger product with many more features. This becomes very clear when Recovery Manager first starts—five icons appear, labeled by task: Back Up Active Directory, Restore AD Objects, Restore AD LDS (ADAM) Objects, Restore Group Policy, Restore Active Directory.

I jumped right in and backed up AD. You can back up each DC separately, back up a specific container in AD, back up an ADAM directory or specific machines via a TEXT file. The backup can be run immediately or scheduled. Finally, you can specify a computer collection where the DCs will reside. This is useful if you want to back up the DCs in a specific AD site and store the backups on a central store within that site.

After you set up the backup and get it scheduled, you can wait for it to run or run it manually via Scheduled Tasks. To test the

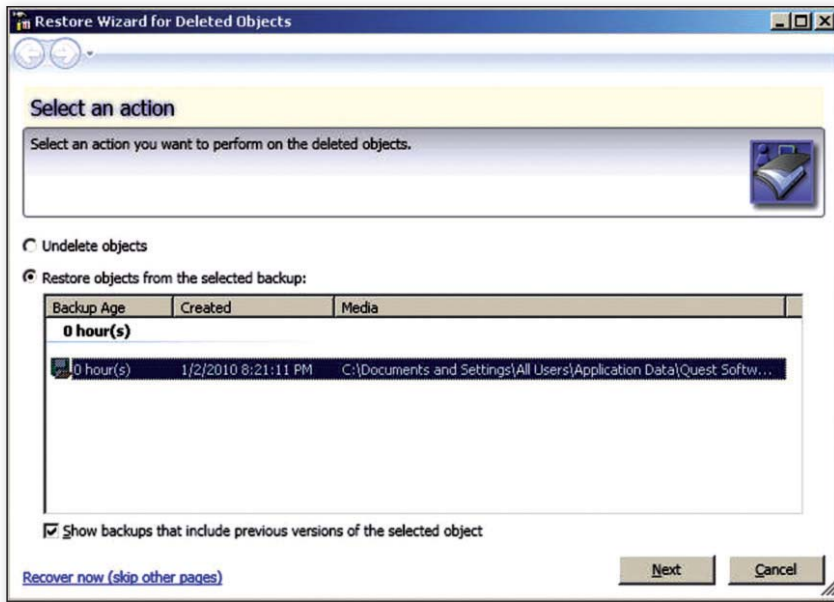


Figure 2: Restoring objects from a backup with Quest Recovery Manager

functionality, I created a couple of users, manually ran the backup (it takes only a few seconds on a small domain), then deleted a user. In Active Directory Users and Computers, I noticed a new Deleted Objects container at the top of the tree. Selecting this container shows all of the objects that have been deleted. I right-clicked the deleted user and chose Recover Deleted Objects.

From this wizard, you could use the built-in recycle bin and simply “undelete” the object; however, as you know, this only recovers the object, not the attributes of the object. So instead I chose *Restore Objects from the Selected backup*, which Figure 2 shows.

Next I needed to choose between an agentless and agent-based method. Recovery Manager’s deployment guide details the advantages and disadvantages of each. In short, the agentless method uses LDAP (which is less intrusive than installing a client), but requires you to extend the AD schema if you want to restore SID history or user passwords. (To learn why SID history can be important, see my article about migrating AD after a company merger, “Plan and Execute an Active Directory Merger, Part 1,” at [windowsitpro.com](http://windowsitpro.com), InstantDoc ID 102596.) An agent-based restore doesn’t require any changes to the schema and is faster than using LDAP. If you choose to use the agent-based method, the agent is installed onto the domain controller (DC) during the

restoration and is automatically removed when complete.

In just a few seconds, the deleted account was restored, along with all of its individual attributes. Note: If you do decide to extend the schema to allow password and SID history recovery without the agent, a simple GUI called Password and SID-History Schema Configuration is provided. Another separate application included with Recovery Manager is the Clone Wizard. If you have ever tried to restore AD onto dissimilar hardware after a disaster (or clone your environment for a lab), you will love this tool.

Recovery Manager is an extremely robust solution that ensures the recovery of everything in your directory structure—from the entire domain down to an individual object. More expensive than the NetWrix product, it also has many more features, such as AD site awareness, DC cloning, Group Policy backup, and direct integration with Active Directory Users and Computers.

### Quest Recovery Manager for Active Directory

**PROS:** Enterprise-caliber AD backup and recovery; super-slick Clone tool makes creating labs and disaster recovery a snap.

**CONS:** Expensive product, might be more than many smaller shops need

RATING: ◆◆◆◆◆

**PRICE:** \$10 per active user; discounts available

**RECOMMENDATION:** If you’re tired of wondering if you could recover your AD infrastructure in the case of a disaster, then get this must-have tool.

**CONTACT:** Quest Software • 800-306-9329 • [www.quest.com](http://www.quest.com)

### Chevy vs. Cadillac

When we do a product review with multiple products, a clear winner is normally chosen and awarded the “Editor’s Choice” designation. However, this works only when you compare apples to apples. These two products are in two different leagues.

NetWrix Active Directory Change Reporter provides great rollback functionality for deleted AD objects that is head-and-shoulders better than the built-in functionality in AD. Its reporting capability and very low cost per active user make it a logical choice for a less complex network in a company on a budget. If your AD is not that complex, consider this Chevy.

Quest Recovery Manager for Active Directory, on the other hand, is a Cadillac designed for larger environments. Its higher sticker price might be a turn-off to some, but before you dismiss it outright, consider the cost and “interruption factor” of a major AD disaster. You might find the additional cost of Recovery Manager to be well worth it.

Support for both products is provided via a Knowledge Base website where you can also open new incidents. Phone support is also available. The choice is yours: Simple and inexpensive, or very robust with a higher price—you can’t go wrong either way.



InstantDoc ID 103641



### Eric B. Rux

([ebrux@whshelp.com](mailto:ebrux@whshelp.com)) is a contributing editor for *Windows IT Pro*, cofounder of [WHSHelp.com](http://WHSHelp.com), and writes a monthly column at [svconline.com/connectedhome/](http://svconline.com/connectedhome/), [windowshomeserver.com](http://windowshomeserver.com). Eric is a senior Windows administrator and teaches the Microsoft Certified Systems Administrator (MCSA) program at a tech college.

# Relieve deployment headaches

**DOWNLOAD A FREE  
30-DAY TRIAL**

The only deployment  
solution with driver  
packages included

Save thousands with  
per-technician licensing

No need to modify  
images for different  
hardware

No need for dedicated  
hardware

No connected services  
required

Manage your entire  
business with a single  
toolset

**WINDOWS IT PRO  
SUBSCRIBERS  
RECEIVE 20% OFF  
THROUGH MAY 2010**



[SMARTDEPLOY.COM/WITP](http://SMARTDEPLOY.COM/WITP) · 1-888-7-DEPLOY





# Windows Password Reset Products

Free up some IT time with a self-service application

by Lavon Peters

In January, data security company Imperva released its *Consumer Password Worst Practices*, in which the company analyzed 32 million exposed passwords. You might not be surprised to learn that the most frequently used passwords are consecutive strings of numbers, letters and numbers (e.g., 123456, abc123), or common words and phrases (e.g., princess, iloveyou, qwerty). And—shockingly—(not really) the fourth most common password is, in fact, the word *password*.

We all know what constitutes a secure password: It doesn't contain any personal or identifying information (user's name, birth date, city, child's name, dog's name), it isn't easy to guess (à la "password"), and it contains unique characters (numbers, both uppercase and lowercase letters, special characters such as an underscore). But getting users to actually employ secure passwords is like pulling teeth. They have a hard time coming up with unique passwords and an even harder time remembering them. If you do convince (or require) your users to create strong passwords, they invariably jot the passwords down on sticky notes that they then attach to their computer monitors. So much for security.

## Strong Passwords

Because insecure passwords have serious security implications in the enterprise, enforcing strong password policies is important. In its password report, Imperva provides some best practices for selecting strong passwords.

- Passwords should have at least eight characters.
- Use a mix of different character types (e.g., upper case, lower case, numbers, special characters). If the password contains only one letter, number, or special character, it shouldn't be the first or last character in the password.
- The password shouldn't be a name, a slang word, or any word that can be found in the dictionary. It also shouldn't contain any part of the user's name or email address.

## Now What Was That Password Again?

Unfortunately, strong passwords are difficult to remember. One of the main drawbacks of enforcing strong password policies is that when a user forgets his or her password, the IT administrator must drop

everything and immediately recover or reset that password. Time wasted because a user has forgotten his or her logon password and can't access the system is lost productivity. However, the time a systems administrator spends every week or month resetting passwords is equally wasteful. A great solution is a password reset product.

Numerous software products exist for automatically resetting Windows passwords. These solutions substantially reduce IT administrator involvement. Users need only answer a series of questions (which in some cases the administrator must initially configure). Some products temporarily reset the password to a random, automatically generated password that the user must then manually reset, whereas other products let the user reset his or her password immediately.

All of the password reset products included in this buyer's guide allow users to reset passwords from the Windows logon screen. Most of the products also provide a web interface for resetting passwords, and a few offer telephone access. Some of the products even generate an email to inform users of impending password expiration.

## Take IT Out of the Picture

The most common call IT administrators receive is to reset users' passwords. In fact, these calls constitute 25 percent of all Help desk requests. No wonder users complain that their IT administrators are slow in responding—if you're running around resetting passwords for 2 hours a day, it's hard to get any real work done. A better solution is to put the power back into users' hands, and free up your IT resources for more important tasks. Consider the password reset products in the accompanying table, or another similar product. The time you save will be well worth the price.



InstantDoc ID 103606



**Lavon Peters** (lpeters@windowsitpro.com) is a senior editor for *Windows IT Pro* and *SQL Server Magazine*, specializing in security. She has worked as a technical editor since 1994.

## PASSWORD RESET PRODUCTS

Company	Product	Price	Windows OSs	Access via:			Temporary Reset?	Expiry Notification?
				Logon Screen?	Web Browser?	Telephone?		
Advanced Software Products Group 239-649-1548 800-662-6090 www.aspg.com	ReACT	\$5,500 per mainframe; \$1,100 per server, plus \$10.50 per user	Windows Server 2008 R2, Server 2008, Windows Server 2003, Windows 2000	Yes	Yes	No	No	No
ANIXIS 240-209-4857 www.anixis.com	ANIXIS Password Reset	\$380 for 50 users; \$3,610 for 1,000 users; \$6,280 for 2,000 users	Windows 7, Server 2008 R2, Server 2008, Windows Vista, Windows 2003, Windows XP, Windows 2000	Yes	Yes	No	No	No (available in Password Policy Enforcer)
Avatier 925-217-5170 800-609-8610 www.avatier.com	Avatier Password Station	Varies, depending on functionality	Windows 7, Server 2008 R2, Server 2008, Vista, Windows 2003, XP, Windows 2000	Yes	Yes	Yes	Yes	Yes
Gold Systems 303-447-2774 800-988-7798 www.goldsys.com	Gold Systems Password Reset	\$29,000	Server 2008 R2, Server 2008, Windows 2003, XP, Windows 2000	Yes	Yes	Yes	Yes	Yes
Hitachi ID Systems 403-233-0740 www.hitachi-id.com	Hitachi ID Password Manager	Varies by volume, from \$6-\$21 per user	Windows 7, Server 2008 R2, Server 2008, Vista, Windows 2003, XP, Windows 2000	Yes	Yes	Yes	No	Yes
NetWrix 201-490-8840 888-638-9749 www.netwrix.com	NetWrix Password Manager	Starting at \$5.50 per user for 150 users; as low as \$1 per user in larger environments	Windows 7, Server 2008 R2, Server 2008, Vista, Windows 2003, XP	Yes	Yes	No	Yes	No (Password Expiration Notifier is optional)
Passlogix 212-825-9100 866-727-7564 www.passlogix.com	v-GO Self-Service Password Reset (SSPR)	\$12 per seat	Windows 7, Server 2008 R2, Server 2008, Vista, Windows 2003, XP	Yes	Yes	No	Yes	No
Specops Software 416-849-5325 877-773-2677 www.specopssoft.com	Specops Password Reset	\$1,400 per domain; starting at \$6 per user	Windows 7, Server 2008 R2, Server 2008, Vista, Windows 2003, XP, Windows 2000	Yes	Yes	No	No	Yes
SysGem +41 (0)44 204 60 23 www.sysgem.com	Sysgem Self-Service Password Reset	Sliding scale; typically \$1 per user for corporate accounts	Windows 7, Server 2008 R2, Server 2008, Vista, XP, Windows 2000	Yes	No	No	Yes	No

**Editor's Note:** Information in this buyer's guide comes from vendor representatives and resources and is meant to jump-start, not replace, your own research; also, some products might have been left out, either as an oversight or from lack of vendor response.

■ SharePoint 2010

■ IT Careers

■ Smartphones

## INSIGHTS FROM THE INDUSTRY

## Discoverability and SharePoint 2010

One of the most obvious changes to SharePoint 2010 is the Ribbon. The Ribbon (also known as the Fluent UI) was introduced in Microsoft Office 2007 and is now common in many Microsoft and third-party applications. Although the initial transition to the Ribbon is indeed a transition, I think that few people would argue against the fact that the Ribbon is a very productive way to organize and make “discoverable” the features of an application. With the Ribbon coming to SharePoint, users and administrators will have easier access to the commands they need and will likely discover new features that would otherwise go unnoticed.

I'd like to share a story of how I decided that, yes, the Ribbon is a great addition to SharePoint. Along the way, I'll point out some new features of SharePoint 2010: in-browser form customization and easy creation of forms for related lists. And I'll lament an all-too-common problem with Microsoft: painfully close but still off-the-mark new features. Unfortunately, Microsoft stopped one important step short of perfect in its implementation of these new features.

As you have probably heard, SharePoint 2010 provides capabilities that let you create relationships between lists. In the classic example, a list of customers can be related to a list of orders. And, in fact, referential integrity can be configured so that if a customer is deleted, for example, the customer's orders can also be deleted.

This relational capability is fantastic, on its own. In Microsoft Office SharePoint Server (MOSS) 2007, you had to do quite a lot of SharePoint Designer and Visual Studio (VS) work to do the same things.

After you complete relating the lists, you typically want to show the list items

and their related data. So, for example, I would want to be able to view a customer and see all of his or her orders. This also required a bit of work in previous versions of SharePoint, and I would pull out SharePoint Designer to do the job.

Enter the Ribbon. As I was creating an application for a client involving related lists, I noticed that on the List tab of the Ribbon, there was a Form Web Parts button that exposed a command: Default Display Form. The beauty of the Ribbon is that this command would have been buried down a submenu in a legacy, menu-driven UI. Here, it jumped out at me as something I could do to the list.

**As you have probably heard, Sharepoint 2010 provides capabilities that let you create relationships between lists.**

As soon as I chose the Default Display Form command, I noticed that the Ribbon exposed a Related Lists button on the Page Tools Insert tab, which would clearly “insert a related list.” Wow... now that is discoverable when someone can naturally stumble upon a great new feature.

I was thrilled to go from being unaware that I could customize the default pages in the web browser—no SharePoint Designer needed—to having a customized page in a matter of minutes, thanks to the discoverability of the Ribbon

UI. What I was not thrilled to discover was that Microsoft stopped one step short on its implementation of the “related lists” views.

If I am looking at a customer, with a view of his or her orders below, and the Orders list has an Add New Item command, why would I click that? Of course, to create a new order for that customer, right? I'd want the new order form to already be “linked” to the customer. In MOSS 2007, you had to do some work—usually by passing parameters in the URL—to tell the new item how to pre-populate a field like “customer.”

Looks like you'll have to do that, somehow, in SharePoint 2010 as well. Unfortunately, the Add New Item command opens the new Order form without pre-populating the Customer ID, leaving the user to populate that field.

That seems like a small gap in functionality, but my experience has been that it's just those kind of “obvious” usability gaps that reduce the perceived value of all the goodness that Microsoft does integrate into its products. I would hope that a Microsoft developer could code a good “pass the parameter to the form” solution for us, so that every customer wouldn't have to figure out how to do it on their own.

On a related note, the Ribbon is not pervasive yet in the public beta of SharePoint 2010. In Central Administration for example, the Ribbon gives beautiful access to commands for web applications, but not for site collections—a glaring gap, in my opinion. Site collections still are managed using the same clumsy “don't forget to change the site collection to the desired one” pages. Maybe this will get corrected before SharePoint is released.

—Dan Holme

InstantDoc ID 103417



# Create Professional, Beautiful Resumes for Free

It's no big secret that job markets seem to get more competitive every day. Simply having the right experience, degrees, and accreditations is no guarantee of success. Everyone is looking for a way to stand out.

Well, I say there's no better way to stand out than with your resume. Resumes are the most boring, monochromatic, cookie-cutter looking creations in the history of job searchers everywhere. Every hiring manager has probably reached a point where he/she wants to set fire to a giant pile of black-and-white documents and watch his/her employee prospects go down in a blaze of glory.

But it doesn't have to be that way. At least, not if people start eyeing BriteTab's resume creation service as an option.

To get started, sign up for free at [www.britetab.com](http://www.britetab.com), then start creating your resume. Choose a template, choose your layout, then plug in the text and go.

**Resumes are the most boring, monochromatic, cookie-cutter looking creations in the history of job searchers everywhere.**

Everything can be created in a very basic, very easy WYSIWYG tool.

## Adding Images and Video

After the text is there, you can easily add images and video to your resume. (There are tutorial videos on adding these elements on the website.) I was able to create a basic resume in about 30 minutes, most of which was playing with the tools. Because it's a web resume, it's also really easy to put hyperlinks in for your blog, Twitter page, or related content.

## Cool, But Will It Help?

That's the question I was asking myself as I started using this tool. Because on one hand, the resumes are pretty pretty, but

on the other hand I wonder if the fascination ends there. When I see one of these resumes, I feel somewhat impressed by the individual but also as though I wouldn't want to hire them. Maybe it seems somehow snobby, or maybe it's just that I'm not used to it.

As a best practice if you do decide to employ this service, I'd recommend also having a classic resume to send out, for hiring managers who want to print out the resume or just want to view it in the more basic format. (And I'm sure you all know to send a PDF, not a Microsoft Word file, right?)

I think that covers everything I want to say about BriteTab. Check it out, build your own resume, and let me know what you think. Email [breinholz@windowsitpro.com](mailto:breinholz@windowsitpro.com) or tweet @breinholz.

—Brian Reinholz

InstantDoc 103494

**Erik Lucien**  
Architect and Construction Manager  
563.555.2452 | [elucien@britetab.com](mailto:elucien@britetab.com)

**Accomplishments and Achievements**

- AIA awards for Phoenix Consolidated Rental Car Facility and Portola Residence
- Management track record that enables revenue and profit growth
- Strong analytical, organizational, leadership, and effective communication skills
- Creative value engineering and subcontractor buyout process
- Licensed CA architect #18033

**KNOWLEDGEABLE, CREATIVE, PRODUCTIVE, and ACCOMPLISHED ARCHITECT and CONSTRUCTION MANAGER:**

Produces design and construction projects as design architect, and has worked as a construction manager, owner's agent and construction project manager for public, speculative development and private clients. Delivers all project tasks in a timely and cost effective manner. Provides comprehensive administration/management services in preconstruction/proposal stages, design, bidding, permitting, contractor selection/negotiation/contracts, construction and closeout stages. Also purchases and installs tenant's FF&E, achieves occupancy, moves tenant and closes out projects.

Continuously seeks creative solutions for problem resolutions throughout project timeline. Personally coordinates with consulting building engineers, project consultants, city planning and building departments to provide quality assurance and all required permits.

**Employment**

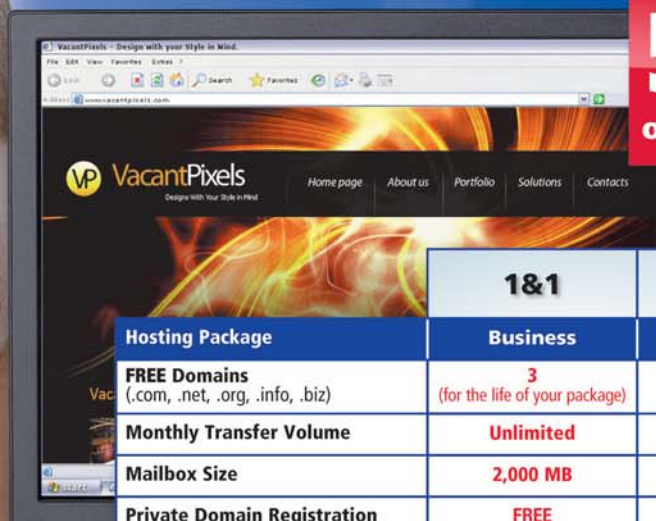
**Devcon Construction, Inc.**  
Sunnyvale, CA  
June 2007 - July 2009

**Project Manager**  
Managed all phases of construction for two five story LEED Silver Class A office buildings. Assisted with overall Sunnyvale Town Center project design review and supervised quality assurance of project, project planning, drawing review, construction permit submittals and revisions, and interface with City of Sunnyvale permit department and field inspectors for office, condo, retail and garage projects.

- Achieved buyout savings of \$8 million on a \$52 million budget for both buildings.

# QUALITY

WEB HOSTING AT THE BEST PRICE!



**6 MONTHS**  
**50% OFF**  
**ON THE 1&1 BUSINESS PACKAGE\***

	<b>1&amp;1</b>	<b>Network Solutions</b>	<b>Go Daddy</b>
Hosting Package	<b>Business</b>	<b>Small</b>	<b>Unlimited</b>
<b>FREE Domains</b> (.com, .net, .org, .info, .biz)	<b>3</b> (for the life of your package)	<b>1</b> (first year only)	—
<b>Monthly Transfer Volume</b>	<b>Unlimited</b>	3,000 GB	<b>Unlimited</b>
<b>Mailbox Size</b>	<b>2,000 MB</b>	1,000 MB	1,000 MB
<b>Private Domain Registration</b>	<b>FREE</b>	\$9.00/year	—
<b>Search Engine Submission</b>	✓	✓	Extra charge applies
<b>Money Back Guarantee</b>	<b>90 days</b>	30 days	—
<b>Special Offer</b>	<b>6 MONTHS</b> <b>50% OFF</b>	—	—
<b>Price Per Month</b>	<del>\$9.99</del> <b>\$4.99</b> for 6 months*	<b>\$9.96</b>	<b>\$14.24</b>
<b>First Year Hosting Total</b> (with discount)	<b>\$89.91/year</b>	<b>\$128.52/year</b>	<b>\$170.88/year</b>

"Working with startup companies on a tight budget, my clients know an online presence is needed. I use 1&1 exclusively to satisfy their requests for reliable hosting at affordable rates."

Lance Ochs, [www.vacantpixels.com](http://www.vacantpixels.com)

As the world's largest web host, with over 20 years of experience and state-of-the-art data centers worldwide, 1&1 is dedicated to security, innovation and value when it comes to your website.



**99.9% Uptime!**



**90-Day Money Back Guarantee!**



**24/7 Toll Free Support**

More special offers are available online. For details, visit [www.1and1.com](http://www.1and1.com)

\*Offer valid as of March 1, 2010. 12 month minimum contract term applies. Setup fee and other terms and conditions may apply. Visit [www.1and1.com](http://www.1and1.com) for full promotional offer details. Program and pricing specifications and availability subject to change without notice. 1&1 and the 1&1 logo are trademarks of 1&1 Internet AG, all other trademarks are the property of their respective owners. © 2010 1&1 Internet, Inc. All rights reserved.



Call **1-877-GO-1AND1**  
Visit us now **[www.1and1.com](http://www.1and1.com)**





## Choosing a Smartphone: The OS

I'm in the market for a smartphone, and I'm hoping that whatever I choose might be an enterprise-standard device for years to come. I've never owned one and had never used one until recently. And here's a more shocking revelation: I do not now nor have I ever owned any type of cell phone. That's right—that's one modern convenience that I've never found convenient.

In addition to covering Microsoft Exchange Server and Outlook topics for *Windows IT Pro*, I'm also responsible for the mobility space. But not having direct experience with mobile devices is somewhat of a hindrance in this regard, so the powers that be here have determined that the company should supply me with such a device. Now all I have to do is figure out what to choose.

The IT department for Penton Media, *Windows IT Pro's* parent company, doesn't limit employees' choice of mobile devices. So within the organization, we've got BlackBerry devices, Windows Mobile devices, PalmOS, even iPhones. The Droid, I was told, is currently on hold because they're having some "email issues" with it, but after they get those kinks worked out, it too will enter the pool. But as I said at the outset, I want the device I get to be an enterprise standard—something you,

our readers, are using and supporting in your businesses on a daily basis. That's where things at this point seem a little cloudy.

**What features are essential in a business smartphone these days? Touch screens and GPS are nice, but are they necessary to get the job done?**

Just starting with the OS, the mobile space seems rather volatile. Obviously, we focus on Windows-based shops, but does that mean you're supporting primarily Windows Mobile devices? I suspect not. Microsoft's mobile OS has fallen well behind in functionality and the coolness factor to BlackBerry, iPhone, and now even Android devices. Windows Mobile 7.0 has been dangling out there for so long that you have to wonder if that carrot will be too shriveled up for anyone to want to bite when it's in reach, no matter how much hype Microsoft can put behind it.

So here's where you can help, readers. I've put together a couple of quick polls, which you can see at [www.windowsitpro.com](http://www.windowsitpro.com), InstantDoc ID 103473. The first one is intended to see how many of you are like my company,

supporting multiple mobile OSs. The second one asks you to predict the future by letting us know what you think might shake out as the leader among mobile OSs in coming years. I plan to use this information to help me determine which smartphone to request.

In the meantime, feel free to share your stories about how your company selects what to support. Is that decision in the hands of the IT department or of end users? Also, what specific features are essential in a business smartphone these days? I mean, touch screens and GPS are nice, but are they necessary to get the job done?

Help me in my quest for the perfect device! Send an email to [bwinstead@windowsitpro.com](mailto:bwinstead@windowsitpro.com) to let me know what you think.

—B. K. Winstead

InstantDoc 103473



### Are Your IIS Servers Under Attack?

## Block all unwanted IIS traffic with ThreatSentry

**download free trial**

- IIS web application firewall & IPS
- stops known, new and internal threats
- blocks sql injection, xss, dos and more
- reinforces regulatory compliance

Microsoft GOLD CERTIFIED Partner | IIS/Software Solutions Data Management Solutions

[sales@privacyware.com](mailto:sales@privacyware.com) • [www.privacyware.com](http://www.privacyware.com) • 732.212.8110 x235



For detailed information about products in this issue of *Windows IT Pro*, visit the web sites listed below.

COMPANY/URL	PAGE	COMPANY/URL	PAGE	COMPANY/URL	PAGE
<b>1&amp;1 Internet</b> .....	69	<b>Microsoft</b> .....	17	<b>Privacyware</b> .....	70
www.1and1.com		www.mms-2010.com		www.privacyware.com	
<b>Diskeeper Corporation</b> .....	4	<b>Microsoft</b> .....	49-54	<b>Prowess Corporation</b> .....	64
www.diskeeper.com/special45daytrial		www.microsoft.com		www.prowess.com	
<b>HOB Inc.</b> .....	Cover 3	<b>Microsoft</b> .....	55	<b>Sunbelt Software Inc.</b> .....	2
www.hobsoft.com/DoD2		www.itseverybodysbusiness.com/virtual		www.TestDriveVipre.com	
<b>IBM Corporation</b> .....	Cover 4	<b>Netwrix Corporation</b> .....	12	<b>Windows IT Pro Magazine</b> ... 7, 10, 24, 30, 38	
www.ibm.com/collaborate		www.netwrix.com		www.windowsitpro.com	
<b>Microsoft</b> .....	Cover 2				
www.itseverybodysbusiness.com/deploy					

## VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

5280 Solutions .....	57	Hitachi ID Systems.....	66	Quest Software.....	62
Advanced Software Products Group .....	66	Laserfiche.....	56	SAFENTRIX .....	56
ANIXIS .....	66	Netwrix .....	61, 66	SecretWeapon Systems.....	57
Apple .....	57	Nexsan.....	56	Specops Software .....	66
Automation Anywhere .....	58	NitroSecurity.....	56	Splunk .....	60
Avatier.....	66	Passlogix.....	66	SysGem .....	66
FileTek .....	56	PJ Technologies .....	59	Zeacom .....	57
Gold Systems.....	66				

## DIRECTORY OF SERVICES | WINDOWS IT PRO NETWORK

Search our network of sites dedicated to hands-on technical information for IT professionals.  
**www.windowsitpro.com**

### Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.

**www.windowsitpro.com/forums**

### News

Check out the current news and information about Microsoft Windows technologies.

**www.wininformant.com**

### EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

*asp.netNOW*

*Exchange & Outlook UPDATE*

*SharepointPro Connections UPDATE*

*Security UPDATE*

*SQL Server Magazine UPDATE*

*DevConnections UPDATE*

*Windows IT Pro UPDATE*

*Windows Tips & Tricks UPDATE*

*WinInfo Daily UPDATE*

**www.windowsitpro.com/email**

### RELATED PRODUCTS

#### Custom Reprint Services

Order reprints of *Windows IT Pro* articles. Diane Madzelonka at Diane.madzelonka@penton.com.

### Super CD/VIP

Get exclusive access to all of our print publications, including *Windows IT Pro*, via the new, banner-free VIP Web site.

**www.windowsitpro.com/sub/vip**

### Article Archive CD

Access every article ever printed in *Windows IT Pro* magazine since September 1995 with this portable and speedy tool.

**www.windowsitpro.com/sub/cd**

### SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.

**www.sqlmag.com**

### ASSOCIATED WEBSITES

#### DevProConnections

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.

**www.devproconnections.com**

#### Office & SharePoint Pro

Dive into Microsoft Office and SharePoint content offered in specialized articles, member forums, expert tips, and Web seminars mentored by a community of peers and professionals.

**www.officesharepointpro.com**

### NEW WAYS TO REACH

#### WINDOWS IT PRO EDITORS:

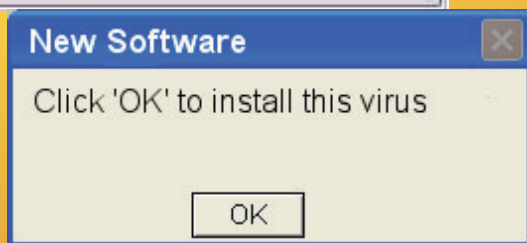
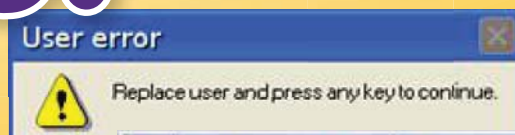
**LinkedIn:** To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage ([www.linkedin.com](http://www.linkedin.com)), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

**Facebook:** We've created a page on Facebook for *Windows IT Pro*, which you can access at: <http://tinyurl.com/d5bquf>. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.

**Twitter:** Visit the *Windows IT Pro* Twitter page at [www.twitter.com/windowsitpro](http://www.twitter.com/windowsitpro).

# Windows IT Pro

# APRIL FOOLS!



## Product of the Month

Our favorite product announcement this month is from the French vendor Be.ez (pronounced "Be Easy"). The company's product—LA robe iPad Allure—claims to bring "Stylish Protection to Apple's New iPad." The company has traditionally offered stylish, protective sleeves for netbooks and MacBooks, but in light of some of the press circulating about the new Apple device's name, we're not sure "protection" is the best word to use for this one! Nevertheless, LA robe iPad Allure protection sleeves will be available this spring for \$29.95. Check out the Be.ez website ([www.be-ez.com](http://www.be-ez.com)).



April 2010 issue no. 188, *Windows IT Pro* (ISSN 1552-3136) is published monthly. Copyright 2010, Penton Media, Inc., all rights reserved. Windows is a trademark or registered trademark of Microsoft Corporation in the United States and/or other countries, and *Windows IT Pro* is used under license from owner. *Windows IT Pro* is an independent publication not affiliated with Microsoft Corporation. Microsoft Corporation is not responsible in any way for the editorial policy or other contents of the publication. *Windows IT Pro*, 221 E. 29th St., Loveland, CO 80538, (800) 793-5697 or (970) 663-4700. Sales and Marketing Offices: 221 E. 29th St., Loveland, CO 80538. Advertising rates furnished upon request. Periodicals Class postage paid at Loveland, Colorado, and additional mailing offices. POSTMASTER: Send address changes to *Windows IT Pro*, 221 E. 29th St., Loveland, CO 80538. SUBSCRIBERS: Send all inquiries, payments, and address changes to *Windows IT Pro*, Circulation Department, 221 E. 29th St., Loveland, CO 80538. Printed in the USA. BPA Worldwide Member.





## HOB RD VPN Desktop-on-Demand

### Don't Go To My PC – Go Directly To Your PC!

With HOB RD VPN Desktop-on-Demand you can access your desktop from anywhere. If your computer has been powered down, you can remotely start it.

#### SSL-encrypted and highly performant

The data are encrypted with SSL, and the default port 443 is used.

The RDP protocol is used for obtaining access with optimum performance.

#### Clientless and platform-independent No administrator rights required

This HOB software is browser-based and platform-independent, meaning you can access your data from Windows, Macs or even Linux machines.

The highly performant RDP Java client HOBLINK JWT is integrated in HOB RD VPN.

#### Easy data transfer and local printer support

When you access your desktop, you can use the clipboard and print or transfer files over the Local Drive Mapping feature.

#### Desktop-on-Demand for Windows, Linux and Mac

The desktop acts as an RDP server for Windows XP, Windows Vista and Windows 7 (Exception: the Home Editions).

Even if your desktop is not running a Windows OS, HOB has a solution: HOB X11Gate for Linux or HOB MacGate for Mac OS X.

These add-on components from HOB allow you to access non-Windows desktops over the highly performant RDP protocol.



## HOB RD VPN *Secure Remote Access*

### The Secure and Comprehensive Remote Access Software Suite!

HOB RD VPN is a software product, not a hosted service. This means your data remains fully in your hands, under your control and nobody else's.

HOB RD VPN also provides:

Remote Desktop Services (RDS)

VDI (Virtual Desktop Infrastructure)

Web Server Gate for accessing internal Web servers

File exchange with Web File Access

VT / SSH as a Java client (ideal for administrators)

HOB PPP Tunnel for universal network access

Standard emulations in Java (3270, 5250, VT, 9750)

**[www.hobsoft.com/DoD2](http://www.hobsoft.com/DoD2)**

**HOB RD VPN is Common Criteria certified\***

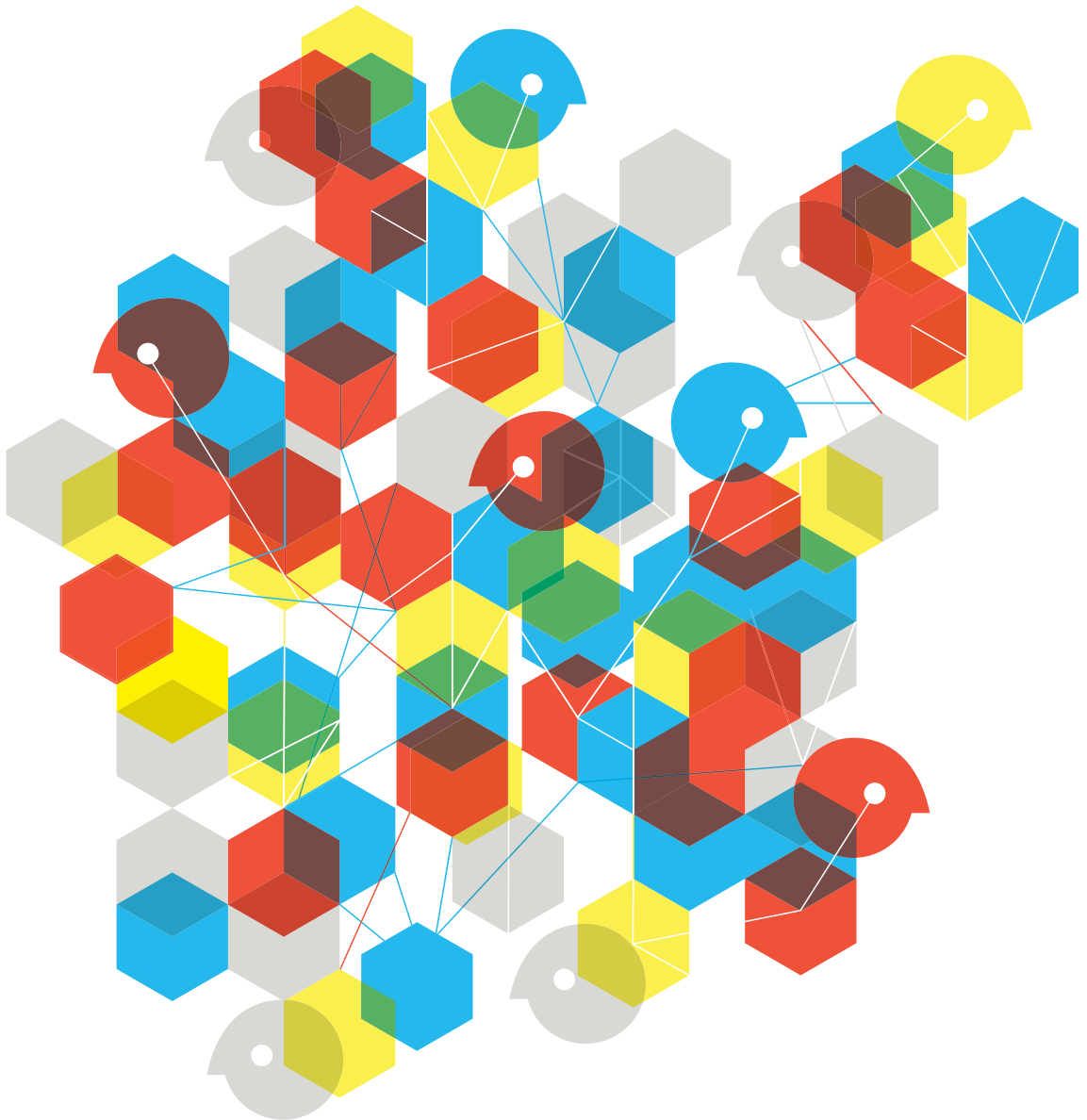


Smarter technology for a Smarter Planet:

## Can the boundaries of a business be defined by its people instead of its walls?

On a smaller, flatter, smarter planet, we increasingly find ourselves working with people far outside the walls of the enterprise: partners, suppliers, customers and remote employees. IBM is incorporating new tools, like social software, wikis and presence awareness, throughout our collaboration portfolio—as well as new ways of accessing these tools through the cloud. Cloud-based solutions like LotusLive™ let your people work with whomever they want, regardless of what side of the firewall they're on. All backed by the legendary security you expect from IBM. Now you can extend your collaboration infrastructure without the cost and complexity of additional infrastructure. So you don't have to tear down your walls to reach beyond them.

A smarter business needs smarter software, systems and services.  
Let's build a smarter planet. [ibm.com/collaborate](http://ibm.com/collaborate)



IBM, the IBM logo, ibm.com, Smarter Planet and the planet icon are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).